95TH CONGRESS } HOUSE OF REPRESENTATIVES { REPORT 95-
2d Session } { 1283, Pt. I

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

JUNE 8, 1978.—Ordered to be printed

Mr. BOLAND, from the Permanent Select Committee on Intelligence, submitted the following

REPORT

together with

SUPPLEMENTAL, ADDITIONAL, AND DISSENTING VIEWS

[To accompany H.R. 7308 which on November 4, 1977, was referred jointly to the Committee on the Judiciary and the Permanent Select Committee on Intelligence]

The Permanent Select Committee on Intelligence, to whom was referred the bill (H.R. 7308) 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, report favorably thereon with amendments and recommend that the bill as amended do pass.

AMENDMENTS

Strike all after the enacting clause and insert in lieu thereof:

That this act may be cited as the "Foreign Intelligence Surveillance Act of 1978".

TABLE OF CONTENTS

29-228

TITLE I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

DEFINITIONS

SEC. 101. As used in this title:

(a) "Foreign power" means—

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

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons; or

(6) an entity that is directed and controlled by a foreign government or governments.

(b) "Agent of a foreign power" means—

(1) any person other than a United States person who—

(A) acts in the United States as an officer, member, or employee of a foreign power; or

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(2) any person who—

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

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; or

(D) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

(c) "International terrorism" means activities that—

(1) involve violent acts or acts dangerous to human life that are or may be a violation of the criminal laws of the United States or of any State, or that might involve a criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended—

(A) to intimidate or coerce a civilian population,

(B) to influence the policy of a government by intimidation or coercion, or

(C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(d) "Sabotage" means activities that involve or may involve a violation of chapter 105 of title 18, United States Code, or that might involve such a violation if committed against the United States.

(e) "Foreign intelligence information" means—

(1) information that relates to and, if concerning a United States person, is necessary to the ability of the United States to protect against—

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

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to and, if concerning a United States person, is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

(f) "Electronic surveillance" means—

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

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

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

(g) "Attorney General" means the Attorney General of the United States (or Acting Attorney General) or the Deputy Attorney General.

(h) "Minimization procedures" with respect to electronic surveillance means—

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition, retention, and dissemination of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1), shall not be disseminated in a manner that identifies any individual United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) Notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for the purpose of preventing the crime or enforcing the criminal law; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 102(a), procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than twenty-four hours unless a court order under section 105 is obtained or unless the Attorney General determines that the

information may indicate a threat of death or serious bodily harm to any person.

(i) "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a) (1), (2), or (3).

(j) "United States", when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(k) "Aggrieved person" means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

(l) "Wire communication" means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

(m) "Person" means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.

(n) "Contents", when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

AUTHORIZATION FOR ELECTRONIC SURVEILLANCE FOR FOREIGN INTELLIGENCE PURPOSES

SEC. 102. (a)(1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that—

(A) the electronic surveillance is solely directed at—

(i) communications exclusively between or among foreign powers, as defined in section 101(a) (1), (2), or (3); or

(ii) the acquisition of technical intelligence from property or premises under the open and exclusive control of a foreign power, as defined in section 101(a) (1), (2), or (3); and

(B) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 101(h); and

if the Attorney General shall report such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least 30 days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.

(2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him.

(3) With respect to electronic surveillance authorized by this subsection, the Attorney General may direct a specified communication common carrier to—

(A) furnish all information, facilities, or technical assistance 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 is providing its customers; and

(B) maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain.

The Government shall compensate, at the prevailing rate, such carrier for furnishing such aid.

(b) Applications for a court order under this title are authorized if the President has, by written authorization, empowered the Attorney General to approve

applications to the Special Court having jurisdiction under section 103, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 105, approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information, except that the Special Court shall not have jurisdiction to grant any order approving electronic surveillance directed solely as described in paragraph (1)(A) of subsection (a) unless such surveillance may involve the acquisition of communications of any United States person.

SPECIAL COURTS

SEC. 103. (a) There is established a Special Court of the United States with jurisdiction throughout the United States to carry out the judicial duties of this title. The Chief Justice of the United States shall publicly designate at least one judge from each of the judicial circuits, nominated by the chief judges of the respective circuits, who shall be members of the Special Court and one of whom the Chief Justice shall publicly designate as the chief judge. The Special Court shall sit continuously in the District of Columbia.

(b) There is established a Special Court of Appeals with jurisdiction to hear appeals from decisions of the Special Court and any other matter assigned to it by this title. The Chief Justice shall publicly designate six judges, one of whom shall be publicly designated as the chief judge, from among judges nominated by the chief judges of the district courts of the District of Columbia, the Eastern District of Virginia and the District of Maryland, and the United States Court of Appeals for the District of Columbia, any three of whom shall constitute a panel for purposes of carrying out its duties under this title.

(c) The judges of the Special Court and the Special Court of Appeals shall be designated for six-year terms, except that the Chief Justice shall stagger the terms of the members originally chosen. No judge may serve more than two full terms.

(d) The chief judges of the Special Court and the Special Court of Appeals shall, in consultation with the Attorney General and the Director of Central Intelligence, establish such document, physical, personnel, or communications security measures as are necessary to protect information submitted to or producted by the Special Court or Special Court of Appeals from unauthorized disclosure.

(e) Proceedings under this title shall be conducted as expeditiously as possible. If any application to the Special Court is denied, the court shall record the reasons for that denial, and the reasons for that denial shall, upon the motion of the party to whom the application was denied, be transmitted under seal to the Special Court of Appeals.

(f) Decisions of the Special Court of Appeals shall be subject to review by the Supreme Court of the United States in the same manner as a judgment of a United States court of appeals as provided in section 1254 of title 28, United States Code, except that the Supreme Court may adopt special procedures with respect to security appropriate to the case.

(g) The Chief Judges of the Special Court and the Special Court of Appeals may, in consultation with the Attorney General and Director of Central Intelligence and consistent with subsection (d)—

(1) designate such officers or employees of the Government, as may be necessary, to serve as employees of the Special Court and Special Court of Appeals; and

(2) promulgate such rules or administrative procedures as may be necessary to the efficient functioning of the Special Court and Special Court of Appeals.

Any funds necessary to the operation of the Special Court and the Special Court of Appeals may be drawn from appropriations for the Department of Justice. The Department of Justice shall provide such fiscal and administrative services as may be necessary for the Special Court and Special Court of Appeals.

APPLICATION FOR AN ORDER

SEC. 104. (a) Each application for an order approving electronic surveillance under this title shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 103. 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 title. It shall include—

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

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

(3) the identity, if known, or a description of the target of the electronic surveillance;

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

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

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

(5) a statement of the proposed minimization procedures;

(6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

(7) 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 the President with the advice and consent of the Senate—

(A) that the certifying official deems the information sought to be foreign intelligence information;

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

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

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 101(e); 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 reasonably be obtained by normal investigative techniques;

(8) a statement of the means by which the surveillance will be affected;

(9) a statement of the facts concerning all previous applications that have been made to any judge under this title involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;

(10) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this title 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; and

(11) whenever more than one electronic, mechanical, or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device.

(b) Whenever the target of the electronic surveillance is a foreign power, as defined in section 101(a) (1), (2), or (3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the application need not contain the information required by paragraphs (6), (7)(E), (8), and (11) of subsection (a), but shall contain such information about the surveillance techniques and communications or other information concerning United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures.

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

(d) The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 105.

ISSUANCE OF AN ORDER

SEC. 105. (a) Upon an application made pursuant to section 104, 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 application 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: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

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

(4) the proposed minimization procedures meet the definition of minimization procedures under section 101(h); and

(5) the application which has been filed contains all statements and certifications required by section 104 and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 104(a)(7)(E) and any other information furnished under section 104(d).

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

(1) specify—

(A) the identity, if known, or a description of the target of the electronic surveillance;

(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed;

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

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

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

(F) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device; and

(2) direct—

(A) that the minimization procedures be followed;

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

(C) that such carrier, landlord, custodian or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and

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

(c) Whenever the target of the electronic surveillance is a foreign power, as defined in section 101(a)(1), (2), or (3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the order need not contain the information required by subparagraphs (C), (D), and (F) of subsection (b)(1), but shall generally describe the information sought the communications or activities to be subjected to the surveillance, and the type of electronic surveillance involved, incuding whether physical entry is required.

(d) (1) 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, except that an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 101(a) (1), (2), or (3), for the period specified in the application or for one year, whichever is less.

(2) Extensions of an order issued under this title may be granted on the same basis as an orignal order upon an application for an extension and new findings made in the same manner as required for an original order, except that an extension of an order under this chapter for a surveillance targeted against a foreign power, as defined in section 101(a) (4), (5), or (6), may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period.

(3) At the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(e) Notwithstanding any other provision of this title, 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 title to approve such surveillance exists,

he may authorize the emergency employment of electronic surveillance if a judge designated pursuant to section 103 is informed by the Attorney General or his designee 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 title is made to that judge as soon as practicable, but not more than twenty-four hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes such emergency employment of electronic surveillance, he shall require that the minimization procedures required by this title 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 and no order is issued approving the surveillance, 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 political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information may indicate a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 103.

(f) Notwithstanding any other provision of this title, officers, employees, or agents of the United States are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to—

(1) test the capability of electronic equipment, if—

(A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

(B) the test is limited in extent and duration to that necessary to determine the capability of the equipment; and

(C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test;

(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if—

(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and

(C) any information acquired by such surveillance is used only to enforce chapter 119 of title 18, United States Code, or section 605 of the Communications Act of 1934, or to protect information from unauthorized surveillance; or

(3) train intelligence personnel in the use of electronic surveillance equipment, if—

(A) it is not reasonable to—

(i) obtain the consent of the persons incidentally subjected to the surveillance;

(ii) train persons in the course of surveillance otherwise authorized by this title; or

(iii) train persons in the use of such equipment without engaging in electronic surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

(C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

(g) Certifications made by the Attorney General pursuant to section 102(a) and applications made and orders granted under this title shall be retained in accordance with the security procedures established pursuant to section 103 for a period of at least ten years from the date of the application.

USE OF INFORMATION

SEC. 106. (a) Information acquired from an electronic surveillance conducted pursuant to this title concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this title. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this title shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this title may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) No information acquired pursuant to this title shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other 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 evidence obtained or derived from such electronic surveillance on the grounds that—

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e) and the Government concedes that information obtained or derived from an electronic surveillance pursuant to the authority of this title as to which the moving party is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding, the Government may make a motion before the Special Court to determine the lawfulness of the electronic surveillance. Unless all the judges of the Special Court are so disqualified, the motion may not be heard by a judge who granted or denied an order or extension involving the surveillance at issue. Such motion shall stay any action in any court or authority to determine the lawfulness of the surveillance. In determining the lawfulness of the surveillance, the Special Court shall, notwithstanding any other law, if the Attorney General files an affidavit under oath with the Special Court that disclosure would harm the national security of the United States or compromise foreign intelligence sources and methods, review in camera the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the Special Court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials if there is a reasonable question as to the legality of the surveillance and if disclosure would likely promote a more accurate determination of such legality, or if such disclosure would not harm the national security.

(g) Except as provided in subsection (f), whenever any motion or request is made pursuant to any statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to surveillance pursuant to the authority of this title or to discover, obtain, or suppress any information obtained from electronic surveillance pursuant to the authority of this title, and the court or other authority determines that the moving pary is an aggrieved person, if the Attorney General files with the Special Court of Appeals an affidavit under oath that an adversary hearing would harm the national security or compromise foreign intelligence sources and methods and that no information obtained from electronic surveillance pursuant to the authority of this title, and this title has been or is about to be used by the Government in the case before the court or other authority, the Special Court of Appeals shall, notwithstanding any other law, stay the proceeding before the other court or authority and review in camera and ex parte the application, order, and such other materials as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, and the Special Court of Appeals still disclose, under appropriate security procedures and protective orders, to the aggrieved person or his attorney portions of the application, order, or other materials relating to the surveillance only if necessary to afford due process to the aggrieved person.

(h) If the Special Court pursuant to subsection (f) or the Special Court of Appeals pursuant to subsection (g) determines the surveillance was not lawfully authorized and conducted, it shall, in accordance with the requirements of the law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the Special Court pursuant to subsection (f) or the Special Court of Appeals pursuant to subsection (g) determines the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(i) Orders granting or denying motions or requests under subsection (h), decisions under this section as to the lawfulness of electronic surveillance, and, absent a finding of unlawfulness, orders of the Special Court or Special Court of Appeals granting or denying disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except the Special Court of Appeals and the Supreme Court.

(j) In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents may indicate a threat of death or serious bodily harm to any person.

(k) If an emergency employment of electronic surveillance is authorized under section 105(e) and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons 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 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.

REPORT OF ELECTRONIC SURVEILLANCE

SEC. 107. In April of each year, the Attorney General shall transmit to the Administrative Office of the United States Courts and to Congress a report setting forth with respect to the preceding calendar year—

(a) the total number of applications made for orders and extensions of orders approving electronic surveillance under this title; and

(b) the total number of such orders and extensions either granted, modified, or denied.

CONGRESSIONAL OVERSIGHT

SEC. 108. On a semiannual basis the Attorney General shall fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence concerning all electronic surveillance under this title. Nothing in this title shall be deemed to limit the authority and responsibility of thosec ommittees to obtain such additional information as they may need to carry out their respective functions and duties.

PENALTIES

SEC. 109. (a) OFFENSE.—A person is guilty of an offense if he intentionally—

(1) engages in electronic surveillance under color of law except as authorized by statute; or

(2) violates section 102(a)(2), 105(e), 105(f), 105(g), 106(a), 106(b), or 106(j) or any court order issued pursuant to this title, knowing his conduct violates an order or this title.

(b) DEFENSE.—(1) It is a defense to a prosecution under subsection (a)(1) that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

(2) It is a defense to a prosecution under subsection (a)(2) that the defendant acted in good faith belief that his actions did not violate any provisions of this title or any court order issued pursuant to this title, under circumstances where that belief was reasonable.

(c) PENALTY.—An offense described in this section is punishable by a fine of not more than $10,000 or imprisonment for not more than five years, or both.

(d) JURISDICTION.—There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

CIVIL LIABILITY

SEC. 110. CIVIL ACTION.—An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 101 (a) or (b)(1)(A), respectively, who has been subjected to an electronic surveillance or whose communication has been disseminated or used in violation of section 109 shall have a cause of action against any person who committed such violation and shall be entitled to recover—

(a) actual damages, but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater;

(b) punitive damages; and

(c) a reasonable attorney's fees and other investigation and litigation costs reasonably incurred.

TITLE II—CONFORMING AMENDMENTS

AMENDMENTS TO CHAPTER 119 OF TITLE 18, UNITED STATES CODE

SEC. 201. Chapter 119 of title 18, United States Code, is amended as follows:

(e) Section 2511(2)(a)(ii) is amended to read as follows:

"(ii) Notwithstanding any other law, communication common carriers, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire or oral communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if the common carrier, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—

"(A) a court order directing such assistance signed by the authorizing judge, or

"(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No communication common carrier, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished an order or certification under this subparagrap, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. No cause of action shall lie in any court against any communication common carrier, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of an order or certification under this subparagraph.".

(b) Section 2511(2) is amended by adding at the end thereof the following new provisions:

"(e) Notwithstanding any other provision of this title or section 605 or 606 of the Communications Act of 1934, it shall not be unlawful 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 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications by a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be

the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.".

(c) Section 2511(3) is repealed.

(d) Section 2518(1) is amended by inserting "under this chapter" after "communication".

(e) Section 2518(4) is amended by inserting "under this chapter" after both appearances of "wire or oral communication".

(f) Section 2518(9) is amended by striking out "intercepted" and inserting "intercepted pursuant to this chapter" after "communication".

(g) Section 2518(10) is amended by striking out "intercepted" and inserting "intercepted pursuant to this chapter" after the first appearance of "communication".

(h) Section 2519(3) is amended by inserting "pursuant to this chapter" after "wire or oral communications" and after "granted or denied".

TITLE III—EFFECTIVE DATE

EFFECTIVE DATE

SEC. 301. The provisions of this Act and the amendments made hereby shall become effective upon the date of enactment of this Act, except 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 this Act, if that surveillance is terminated or an order approving that surveillance is obtained under title I of this Act within ninety days following the designation of the chief judges pursuant to section 103 of this Act.

Amend the title so as to read:

A bill to authorize electronic surveillance to obtain foreign intelligence information.

HISTORY OF THE BILL

In 1976, the Ford administration under the leadership of Attorney General Levi took the revolutionary step of supporting legislation to require a judicial warrant for foreign intelligence electronic surveillances in the United States. While bills which would have created such a requirement had been introduced in the House and Senate each year since 1973, previous administrations' responses were emphatically negative. As then Assistant Attorney General Henry Peterson testified in 1974 before the House Judiciary Committee, "let me be very brief. We oppose these bills. That is it." Attorney General Levi, however, working closely with leaders of the House and Senate, drafted a bill which was introduced in both the House and Senate in 1976 with broad bipartisan support. That bill, as amended, was favorably reported by the Senate Judiciary and Intelligence Committees in 1976, but the session ended before the full Senate could act on the legislation.

The Carter administration, and especially Attorney General Bell, again working closely with House and Senate leaders, picked up where the Ford administration left off, supporting the introduction of a new bill, S. 1566 in the Senate and H.R. 7308 in the House, on May 18, 1977. The Senate bill was favorably reported with amendments by the Senate Judiciary Committee on November 15, 1977, and by the Senate Intelligence Committee on March 14, 1978. S. 1566 was passed by the Senate on April 20, 1978, by a vote of 95–1. In the House, the bill, H.R. 7308, was referred to the Committee on the Judiciary. With

the creation of the Permanent Select Committee on Intelligence, the bill was referred by unanimous consent to this committee as well.

Four days of open hearings were held by the Subcommittee on Legislation. One day of closed hearings was held to obtain classified information concerning the subject area of the bill. Eighteen witnesses were heard in open session, including Attorney General Griffin B. Bell; Director of Central Intelligence, Stansfield Turner; John Shattuck and Jerry Berman of the American Civil Liberties Union; Prof. Lewis H. Pollak, dean of the University of Pennsylvania Law School; Morton Halperin of the Center for National Security Studies; Prof. Arthur Miller of the National Law Center of the George Washington University; Philip Lacovara, former Assistant Special Prosecutor; John S. Warner, Legal Adviser to the Association of Former Intelligence Officers; and Carl H. Imlay, General Counsel of the Administrative Office of the U.S. Courts. While most of these witnesses expressed criticism of certain provisions of H.R. 7308, as introduced, and offered proposed amendments, only three witnesses—Laurence Silberman, former Deputy Attorney General, Representaitive Robert F. Drinan, and Representaitve Charles E. Wiggins—testified in total opposition to H.R. 7308.

The bill, as reported, reflects several major amendments to H.R. 7308 as well as a number of less substantial amendments.

Position of the Administration

The Administration supported the enactment of H.R. 7308, as introduced, in the strongest terms. As Attorney General Bell testified:

> . . . I cannot stress too much the importance of the enactment of this legislation . . . If enacted, the bill would stand as a significant monument to our national commitment to democratic control of intelligence functions and would spur the completion of charter legislation.
>
> As President Carter noted, when he announced this bill, "one of the most difficult tasks in a free society like our own is the correlation between adequate intelligence to guarantee our nation's security on the one hand, and the preservation of basic human rights on the other." It is a very delicate balance to strike, but one which is necessary in our society.
>
> In my view, this bill strikes the proper balance. It sacrifices neither our security nor our civil liberties, and assures that the dedicated and patriotic men and women who serve this country in intelligence positions will have the affirmation of Congress that their activities are proper and necessary.[1]

The administration has noted objections to a small number of this committee's amendments to H.R. 7308. Despite these objections, the administration continues to support passage of the bill.

[1] Hearings before the Subcommittee on Legislation of the House Permanent Select Committee on Intelligence, Hearings on the Foreign Intelligence Electronic Surveillance Bills, 95th Cong., 2d Sess. p. — (1978).

General Statement

I. BACKGROUND

The history and law relating to electronic surveillance for "national security" purposes have revolved around the competing demands of the President's constitutional powers to gather intelligence deemed necessary to the security of the nation and the requirements of the fourth amendment. The U.S. Supreme Court has never expressly decided the issue of whether the President has the constitutional authority to authorize warrantless electronic surveillance for foreign intelligence purposes. Whether or not the President has an "inherent power" to engage in or authorize warrantless electronic surveillance and, if such power exists, what limitations, if any, restrict the scope of that power, are issues that have troubled constitutional scholars for decades.

In 1928, the Supreme Court, in *Olmstead* v. *United States*, held that wiretapping was not within the coverage of the fourth amendment. Three years later, Attorney General William D. Mitchell authorized telephone wiretapping upon the personal approval of bureau chiefs of syndicated bootleggers and in "exceptional cases where the crimes are substantial and serious, and the necessity is great and [the bureau chief and the Assistant Attorney General] are satisfied that the persons whose wires are to be tapped are of the criminal type." These general guidelines governed the Department's practice through the thirties and telephone wiretapping was considered to be an important law enforcement tool.

Congress placed the first restrictions on wiretapping in the Federal Communications Act of 1934, which made it a crime for any person "to intercept and divulge or publish the contents of wire and radio communications." [2] The Supreme Court construed this section to apply to Federal agents and held that evidence obtained from the interception of wire and radio communications, and the fruits of that evidence, were inadmissible in court.[3] However, the Justice Department did not interpret the Federal Communications Act or the *Nardone* decision as prohibiting the interception of wire communications per se; rather only the interception and divulgence of their contents outside the Federal establishment was considered to be unlawful. Thus, the Justice Department found continued authority for its national security wiretaps.

In 1940, President Roosevelt issued a memorandum to the Attorney General stating his view that electronic surveillance would be proper under the Constitution where "grave matters involving defense of the nation" were involved. The President authorized and directed the Attorney General "to secure information by listening devices [directed at] the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies." The Attorney General was requested "to limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens."

[2] 47 U.S.C. 605 (1964 ed.) 48 Stat. 1103.
[3] *Nardone* v. *United States*, 302 U.S. 379 (1937) ; 308 U.S. 338 (1939).

This practice was continued in successive administrations. In 1946, Attorney General Tom C. Clark ent President Truman a letter informing him of President Roosevelt's directive. Clark's memorandum, however, omitted the portion of President Roosevelt's directive limiting wiretaps "insofar as possible to aliens." Instead, he recommended that the directive "be continued in force" in view of the "increase in subversive activities" and "a very substantial increase in crime." President Truman approved.[4]

In the early fifties, however, Attorney General J. Howard McGrath took the position that he would neither approve nor authorize microphone surveillances by means of trespass. This position was quickly reversed by Attorney General Herbert Brownell in 1954 in a sweeping memorandum to FBI Director Hoover instructing him that the Bureau was indeed authorized to conduct such microphone surveillances regardless of the fact of surreptitious entry and without the need to first acquire the Attorney General's authorization. Such surveillance was simply authorized whenever the Bureau concluded that the "national interest" so required. The Brownell memorandum is instructive:

> It is my opinion that the department should adopt that interpretation which will permit microphone coverage by the FBI in a manner most conducive to our national interest. I recognize that for the FBI to fulfill its important intelligence function, considerations of internal security and the national interest are paramount; and, therefore, may compel the unrestricted use of this technique in the national interest.

From the relatively limited authorization of warrantless electronic surveillance under President Roosevelt, then, the mandate for the FBI was expanded to the point where the criterion was the FBI's judgment that the "national interest" required the electronic surveillance.

The practice of the Bureau during the fifties was also described in a memorandum from Director Hoover to the Deputy Attorney General on May 4, 1961:

> [I]n the internal security field, we are utilizing microphone surveillance on a restricted basis even though trespass is necessary to assist in uncovering the activities of Soviet intelligence agents and Communist party leaders. In the interests of national safety, microphone surveillances are also utilized on a restricted basis, even though trespass is necessary, in uncovering major criminal activities. We are using such coverage in connection with our investigations of the clandestine activities of top hoodlums and organized crime. From an intelligence standpoint, this investigative technique has produced results unobtainable through other means. The information so obtained is treated in the same manner as information obtained from wiretaps, that is, not from the standpoint of evidentiary value but for intelligence purposes.

[4] In 1950, aides to President Truman discovered Clark's incomplete quotation, and the President considered returning to the terms of the original 1940 authorization. However, the 1946 directive was never rescinded. See, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (Church Committee), *Final Report*, book II, Page 60.

The policy of the Department of Justice was stated publicly in 1966 by the Solicitor General in a supplemental brief to the Supreme Court in *Black* v. *United States*.[5] Referring to the general delegation of authority by Attorneys General to the Director of the Bureau, the Solicitor stated:

> An exception to the general delegation of authority has been prescribed, since 1940, for the interception of wire communications, which (in addition to being limited to matters involving national security or danger to human life) has required the specific authorization of the Attorney General in each instance. No similar procedure existed until 1965 with respect to the use of devices such as those involved in the instant case, although records of oral and written communications within the Department of Justice reflect concern by Attorneys General and the Director of the Federal Bureau of Investigation that the use of listening devices by agents of the Government should be confined to a strictly limited category of situations.
>
> Under departmental practice in effect for a period of years prior to 1963, and continuing until 1965, the Director of the Federal Bureau of Investigation was given authority to approve the installation of devices such as that in question for intelligence (and not evidentiary) purposes which were required in the interests of internal security or national safety, including organized crime, kidnappings and matters wherein human life might be at stake. . . .
>
> Present departmental practice, adopted in July 1965 in conformity with the policies declared by the President on June 30, 1965, for the entire Federal establishment, prohibits the use of such listening devices (as well as the interception of telephone and other wire communications) in all instances other than those involving the collection of intelligence affecting the national security. The specific authorization of the Attorney General must be obtained in each instance when this exception is invoked.

In *Katz* v. *United States*, 389 U.S. 347 (1967), the Supreme Court finally discarded the *Olmstead* doctrine and held that the fourth amendment did apply to electronic surveillance. The Court explicitly declined, however, to extend its holding that the fourth amendment required a warrant for electronic surveillance to cases "involving the national security." 389 U.S. at 358, n. 23. The next year, Congress followed suit: responding to the *Katz* case, Congress enacted the Omnibus Crime Control and Safe Streets Act.

Title III of that act established a procedure for the judicial authorization of electronic surveillance for the investigation and prevention of specified types of serious crimes and the use of the product of such surveillance in court proceedings. It prohibited wiretapping and electronic surveillance by persons other than duly authorized law enforcement officers, personnel of the Federal Communications Commission, or communication common carriers monitoring communications in the normal course of their employment.

[5] 385 U.S. 26 (1966).

Title III, however, disclaimed any intention of legislating in the national security area. The act contained a proviso in section 2511(3) stating:

> 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 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 clear and present danger to the structure or existence of the Government.

Against this background the Supreme Court decided the *Keith* [6] case in 1972. The issue there was narrowly drawn—"the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in *internal security matters* without prior judicial approval." (emphasis added) [7]

The Court took notice of the long-standing Justice Department policy of warrantless electronic surveillance. It also recognized the "elementary truth" that "unless Government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered." [8] In balancing the constitutional rights involved against the governmental objectives, the Court noted the "convergence of first and fourth amendment values not ordinarily present in cases of 'ordinary' crime." [9] The Court went on to pose the issue:

> If the legitimate need of the Government to safeguard domestic security requires the use of electronic surveillance the question is whether the needs of citizens for private and free expression may not be better protected by requiring a warrant before such surveillance is undertaken. We must ask whether a warrant requirement would unduly frustrate the efforts of Government to protect itself from acts of subversion and overthrow directed against it.[10]

In concluding that a warrant was required in *domestic security* surveillance cases, the Court emphasized the traditional reasons for requiring a warrant:

> Fourth amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the executive branch. The fourth amendment does not contemplate the executive officers of the Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the fourth Amendments accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." [11]

[6] *United States* v. *United States District Court*, 407 U.S. 297 (1972).
[7] 407 U.S., at 301.
[8] 407 U.S., at 312.
[9] 407 U.S., at 313.
[10] 407 U.S., at 315.

The Court then went on to consider and reject the Government's argument that the disclosure of information in a warrant application posed the serious danger of leaks and the Government's argument that "internal security matters are too subtle and complex for judicial evaluation." [12] The Court observed that "[c]ourts regularly deal with the most difficult issues of our society. There is no reason to believe the Federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases." [13] As to the secrecy claim, the Court observed the "[t]he investigation of criminal activity has long involved imparting sensitive information to judicial officers who have respected the confidentialities involved." [14]

Finally, the Court rejected the distinction, stressed by the Government, between surveillance for law enforcement purposes and surveillance designed to obtain intelligence relating to domestic threats to national security. The Court responded that official surveillance, whether its purpose is criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy and speech.

However, the Court emphasized that "this case involves only the *domestic* aspects of national security. We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents." [15]

And, in construing the effect of the Title III presidential disclaimer the court wrote: [16]

> Section 2511(3) certainly confers no power, as the language is wholly inappropriate for such a purpose. It merely provides that the Act shall not be interpreted to limit or disturb such power as the President may have under the Constitution. In short, Congress simply left presidential powers where it found them. . . . [W]e therefore think the conclusion inescapable that Congress only intended to make clear that the Act simply did not legislate with respect to national security surveillances.

Since the *Keith* case, four circuit courts of appeals have addressed the question the Supreme Court reserved. The fifth circuit in *United*

[11] 407 U.S., at 316–317. (Footnotes and citations omitted.)
[12] 407 U.S., at 320.
[13] 407 U.S., at 320.
[14] 407 U.S., at 320–321.
[15] 407 U.S., at 321–322.
[16] 407 U.S., at 303, 306.

States v. *Brown*, 484 F.2d 418 (5th Cir. 1973), cert. denied, 415 U.S. 960 (1974), upheld the legality of a surveillance in which the defendant, an American citizen, was incidentally overheard as a result of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes. The court found that on the basis of

> the President's constitutional duty to act for the United States in the field of foreign affairs, and his inherent power to protect national security in the conduct of foreign intelligence.[17]

In *United States* v. *Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc), cert. denied *sub nom. Ivanov* v. *United States*, 419 U.S. 881 (1974), the third circuit similarly held that electronic surveillance conducted without a warrant would be lawful so long as the primary purpose was to obtain foreign intelligence information. The court found that such surveillance would be reasonable under the fourth amendment without a warrant even though it might involve the overhearing of conversations.

However, in *Zweibon* v. *Mitchell*, 516 F.2d 594 (D.C. Cir. 1975), cert. denied, 425 U.S. 944 (1976), the Circuit Court of Appeals for the District of Columbia, in the course of an opinion requiring that a warrant must be obtained before a wiretap is installed on a domestic organization that is neither the agent of, nor acting in collaboration with, a foreign power, questioned whether any national security exception to the warrant requirement would be constitutionally permissible.

Although the holding of *Zweibon* was limited to the case of a domestic organization without ties to a foreign power, the plurality opinion of the court—in legal analysis closely patterned on *Keith*—concluded "that an analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional." [18]

Finally, in *United States* v. *Buck*, 548 F.2d 871 (9th Cir. 1977), the ninth circuit followed *Brown* and *Butenko*, referring to warrantless surveillance of foreign powers and agents of foreign powers as a "recognized exception to the general warrant requirement."

On the basis of the three circuit court decisions upholding the power of the President in certain circumstances to authorize electronic surveillance without a warrant, and in the absence of any court holding to the contrary, the Justice Department firmly maintains that in the absence of legislation, such warrantless surveillances are constitutional.

Thus, after almost 50 years of case law dealing with the subject of warrantless electronic surveillance, and despite the practice of warrantless foreign intelligence surveillance sanctioned and engaged in

[17] 484 F.2d at 426.

[18] 516 F.2d at 613–614. Neither *Brown* nor *Butenko* provide a systematic analysis of the problem within the framework indicated by the Supreme Court decision in *Keith*, i.e., whether the requirement of a warrant would unduly frustrate the exercise of the President's responsibility in the area of national security. The court's opinion in *Brown* simply confirmed the President's inherent power to authorize foreign intelligence collection through, among other things, electronic surveillance without a warrant. The *Butenko* opinion offers a slightly more extensive analysis of the problem. On the other hand, the *Zweibon* opinion, insofar as it considered and rejected the arguments for the existence of an inherent power by applying the analytical framework used by the Supreme Court in *Keith*, was a plurality opinion.

by nine administrations, constitutional limits on the President's powers to order such surveillances remains an open question.

II. STATEMENT OF NEED

As the above indicates, the development of the law regulating electronic surveillance for national security purposes has been uneven and inconclusive. This is to be expected where the development is left to the judicial branch in an area where cases do not regularly come before it.[19] Moreover, the development of standards and restrictions by the judiciary with respect to electronic surveillance for foreign intelligence purposes accomplished through case law threatens both civil liberties and the national security because that development occurs generally in ignorance of the facts, circumstances, and techniques of foreign intelligence electronic surveillance not present in the particular case before the court.

Yet the circumstances which ultimately determine the reasonableness of a search—the nature, circumstances, and purpose of the search, the threat it is intended to address, and the technology involved—are in this area largely hidden from the public view, and the tiny window to this area which a particular case affords provides inadequate light by which judges may be relied upon to develop case law which adequately balances the rights of privacy and national security.

In the past several years, abuses of domestic national security surveillances have been disclosed. This evidence alone should demonstrate the inappropriateness of relying solely on executive branch discretion to safeguard civil liberties. This committee is well aware of the substantial safeguards respecting foreign intelligence electronic surveillance currently embodied in classified Attorney General procedures, but this committee is also aware that over the past thirty years there have been significant changes in internal executive branch procedures, and there is ample precedent for later administrations or even the same administration loosening previous standards. Even the creation of intelligence oversight committee should not be considered a sufficient safeguard, for in overseeing classified procedures the committees respect their classification, and the result is that the standards for and limitations on foreign intelligence surveillances may be hidden from public view. In such a situation, the rest of the Congress and the American people need to be assured that the oversight is having its intended consequences—the safeguarding of civil liberties consistent with the needs of national security. While oversight can be, and the committee intends it to be, an important adjunct to control of intelligence activities, it cannot substitute for public laws, publicly debated and adopted, which specify under what circumstances and under what restrictions electronics surveillance for foreign intelligence purposes can be conducted.

Finally, the decision as to the standards governing when and how foreign intelligence electronic surveillances should be conducted is and should be a political decision, in the best sense of the term, because it involves the weighing of important public policy concerns—civil liber-

[19] See generally Lacovara, "Presidential Power to Gather Intelligence," 40 Law & Contemp. Prob. 106 (1976).

ties and the national security. Such a political decision is one properly made by the political branches of Government together, not adopted by one branch on its own and with no regard for the other. Under our Constitution legislation is the embodiment of just such political decisions.

At least one witness before the Subcommittee on Legislation specifically raised the question of the need for electronic surveillance for foreign intelligence purposes at all. This committee has not assumed that need. Rather, since its formation, the committee has become acquainted with the various techniques that will be subject to this bill, their targets, their product, and the risks involved—both from civil liberties and intelligence standpoint. On the basis of this knowledge, the committee is confident that a real and substantial need for foreign intelligence electronic surveillance—at least under certain defined circumstances—exists. In drafting this bill, the committee has carefully weighed the need against the privacy and civil liberties interests. In some cases, the balance results in an absolute prohibition of surveillance, for example, where a United States citizen is not an agent of a foreign power. In others, surveillance is allowed but subject to strict and rigorous approval and oversight mechanisms. In still others, the need is so great and the privacy interests so small that substantially more flexibiilty is called for. In each circumstance in which surveillance is authorized by this bill, however the committee has determined that a real need exists for surveillance in that circumstance, and that this need outweighs the privacy interests involved.

III. SUMMARY OF LEGISLATION

H.R. 7308, as amended, would enact a new law entitled the "Foreign Intelligence Surveillance Act of 1978." The purpose of the bill is to provide a statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes. The procedures in the bill would be the exclusive means by which electronic surveillance, as defined, could be used for foreign intelligence purposes. The following techniques of electronic surveillance would fall within the bill's prescriptions:

(*a*) The acquisition of a wire or radio communication sent to or from the United States by intentionally targeting a known United States person in the United States under circumstances in which the person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

(*b*) A wiretap in the United States to intercept a wire communication, such as a telephone or telegram communication;

(*c*) The acquisition of private radio tranmissions where all of the communicants are located within the United States; or

(*d*) The use in the United States of any electronic, mechanical or other surveillance device to acquire information other than from a wire communication or radio communication under circumstances in which the person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

H.R. 7308, as amended, creates a Special Court in Washington, D.C., composed of at least one judge designated by the Chief Justice

from each of the judicial circuits and a Special Court of Appeals composed of six judges designated by the Chief Justice from the greater Washington, D.C., area.

The bill would require a prior judicial warrant for all electronic surveillance for foreign intelligence purposes with three limited exceptions. First, where certain types of electronic surveillance are targeted against certain types of foreign powers, under circumstances where it is extremely unlikely that a United States person's communication would be intercepted, no warrant is required. Instead, Attorney General approval is required. Second, emergency surveillance without a warrant would be permitted in limited circumstances, but a warrant would have to be obtained within 24 hours of the initiation of the surveillance. Third, surveillance solely for the purposes of testing equipment, training personnel, or "sweeps" to discover unlawful electronic surveillance are authorized without a warrant under rigorous controls to insure that no information concerning United States persons is improperly used, retained, or disseminated.

The bill would authorize the Attorney General to make applications to the Special Court for a court order approving the use of electronic surveillance. Approval of an application under the bill would require a finding by a judge that the target of the surveillance is either a "foreign power" or an "agent of a foreign power," terms defined in the bill, and that the facilities or places at which the surveillance is directed are being used or are about to be used by a foreign power or agent of a foreign power. A "foreign power" may include a foreign government, a faction of a foreign government, a group engaged in international terrorism, a foreign-based political organization, or an entity directed and controlled by a foreign government or governments, An "agent of a foreign power" includes non-resident aliens who act in the United States as officers, members, or employees of foreign powers or who act on behalf of foreign powers which engage in clandestine intelligence activities in the United States contrary to the interests of this country. U.S. persons meet the "agent of a foreign power" criteria if they engage in certain activities on behalf of a foreign power which involve or may involve criminal acts.

The court would also be required to find that procedures proposed in the application adequately minimize the acquisition, retention, and dissemination of information concerning U.S. persons consistent with the need of the United States to obtain, produce and disseminate foreign intelligence information.

Every application for an order must contain a certification or certifications made 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 with responsibilities for national security or defense who are appointed by the President with the advice and consent of the Senate. Those officials would be required to certify that any information sought by the surveillance relates to, and if concerning a U.S. person is necessary to, the national defense or the conduct of foreign affairs of the United States or the ability of the United States to protect against grave hostile acts or the terrorist, sabotage, or clandestine intelligence activities of a foreign power. The court would be required to review each certification for surveil-

lance of a U.S. person and to determine that the certification is not clearly erroneous.[20]

The court could approve electronic surveillance for foreign intelligence purposes for a period of 90 days or, in the case of surveillance of a foreign government, faction, or entity openly controlled by a foreign government, for a period of up to 1 year. Any extension of the surveillance beyond that period would require a reapplication to the court and new findings as required for the original order.

H.R. 7308 requires annual reports to the Administrative Office of the U.S. Courts and to the Congress of statistics regarding applications and orders for electronic surveillance. The Attorney General is also required, on a semiannual basis, to inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence fully concerning all electronic surveillance under the bill; and nothing in the bill restricts the authority of those committees to obtain further information related to their congressional oversight responsibilities.

IV. CONCLUSION

The purpose of the Foreign Intelligence Surveillance Act is to provide legislative authorization for and regulation of all electronic surveillance conducted within the United States for foreign intelligence purposes. In so doing, the bill does not recognize, ratify, or deny the existence of any Presidential power to authorize warrantless surveillances in the United States in the absence of the legislation. It would, rather, moot the debate over the existence or non-existence of this power, because no matter whether the President has this power, few have suggested that his power would be exclusive. Rather, as two Attorneys General have testified, Congress also has power in the foreign intelligence area. Given the fact that Congress created the Central Intelligence Agency, delimiting its authorized functions and jurisdiction, and appropriates funds for the entire intelligence community, there can be little debate as to the fact that Congress has at least concurrent authority to enable it to legislate with regard to the foreign intelligence activities of departments and agencies of this Government either created or funded by Congress. Thus, even if the President has the inherent authority in the absence of legislation to authorize warrantless electronic surveillance for foreign intelligence purposes, Congress has the power to regulate the conduct of such surveillance by legislating a reasonable procedure, which then becomes the exclusive means by which such surveillance may be conducted. This analysis has been supported by two successive Attorneys General and draws directly from Justice Jackson's famous concurring opinion in the *Steel Seizure Cases*.[20a]

A basic premise behind this bill is the presumption that whenever an electronic surveillance for foreign intelligence purposes may involve the fourth amendment rights of any U.S. person, approval for such a surveillance should come from a neutral and impartial magistrate. This premise has not been adopted without debate and consideration within the committee, as the Minority views will attest.

In approaching this issue, one must begin with the Constitution. What does it mandate? As noted above, this is a question about which reasonable men can certainly differ. While the weight of the case law suggests that a judicial warrant may not be required in certain cases, a plurality of the District of Columbia Circuit has suggested that a warrant is required by the fourth amendment in all cases. Because the Supreme Court has not addressed the issue, and indeed has taken pains not to address the issue, the question must be considered unresolved.

Beyond the constitutional question, there is also a question of proper policy. The minority views reflect the belief that the judiciary should not be involved in foreign intelligence surveillances. With all due respect to those views, the committee's conclusion, shared by the last two administrations involving both political parties, is that a warrant requirement for electronic surveillance for foreign intelligence purposes will not pose unacceptable risks to national security interests and will remove any doubt as to the lawfulness of such surveillance. By requiring a judge ultimately to approve foreign intelligence electronic surveillances, the bill would require the responsible officials in the executive branch to consider and articulate the facts and their appraisal of the facts. If the executive officials were the approving authority, the same consideration and articulation would not be as likely to occur. The experience under title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C., section 2510 et seq., is instructive. While few orders for law enforcement electronic surveillances have been denied, the committee believes that the reason is the care and scrutiny which applications receive before they ever go to a judge. The institutional response to an outside approval authority, then, is to make every effort that only good applications should go to the approval authority.

Moreover, there is no validity to the assertion that judges will somehow become involved under the bill in making foreign policy of foreign intelligence policy. The bill was carefully crafted to prevent such an eventuality. The role of judges under the bill is the same as that of judges under existing law enforcement warrant procedures. That is, judges determine whether the facts presented to them satisfy the statutory criteria. They do not make substantive judgments as to the propriety of or need for a particular surveillance; rather, Congress by enacting this bill establishes the substantive standards as to what the proper target of a surveillance is, what information sought justifies a surveillance, and what standards apply to the retention and dissemination of information obtained. Judges, of course, assess the facts to determine whether certain of the substantive standards have been met, but this is the traditional role of a judge in passing on a warrant application. And while certain of the determinations made by judges under this bill are unique to this area, the same could have been said with respect to title III when it was introduced. Indeed, as searches differ in technique and purpose, differing determinations necessarily

[20] The committee bill contains no general requirement of subsequent notice to the surveillance target, as does section 2518(8)(d) of title 18 for law enforcement surveillances. Such notice is particularly inappropriate in the area of foreign intelligence surveillances, where prosecution is rarely the objective or result. The mere knowledge of the existence or target of a foreign intelligence surveillance would most likely alert foreign governments and espionage services to ongoing U.S. intelligence activities or investigations and compromise sensitive intelligence sources and methods.

[20a] *Youngstown Sheet & Tube* v. *Sawyer*, 343 U.S. 579 (1952).

become involved, but it must be remembered that under this bill judges only make determinations specified by Congress, reflecting these different purposes, and those determinations are solely to apply facts to a statutory standard.

This committee does not expect or desire the judges involved in these determinations to become expert in foreign policy matters or foreign intelligence activities; such expertise would be meaningless under the bill, for there is no opportunity for its utilization.

Some have suggested that even if United States citizens should be protected by a warrant requirement, this protection should not be extended to aliens, non-resident aliens, or diplomatic personnel. Leaving aside the constitutional question whether such persons are entitled to the protection of a prior judicial warrant under the fourth amendment, the purpose of requiring a warrant for the targeting of all electronic surveilance in the United States would not be primarily to protect such persons but rather to protect U.S. citizens who may be involved with them and to ensure that the safeguards inherent in a judicial warrant cannot be avoided by a determination as to a person's citizenship.

Notwithstanding the committee's conclusion that generally a judicial warrant should be required for foreign intelligence surveillances in the United States, in the course of the committee's hearings and discussions it was determined that a certain narrow class of surveillances did not affect the rights of U.S. citizens in any way. Moreover, this class of surveillances is among the most sensitive and important class of surveillances this Government conducts in the United States. These factors led the committee to amend H.R. 7308 so as not to require a judicial warrant in this class of surveillances. The fact that Americans' civil and constitutional rights were not affected by these surveillances, when weighed against even the incremental risk to security by including courts in the approval process, suggested that the benefits of a warrant requirement in such cases were outweighed by its potential risks.

The fact that a warrant is not required in this limited class of cases does not mean, however, that Congress is recognizing or ratifying an inherent power of the President to engage in warrantless electronic surveillance for foreign intelligence purposes. Under H.R. 7308, as amended, the authority of the President to engage in surveillance in certain cases without a warrant will derive from statute, not the Constitution, and it will be subject to the limitations and requirements of the bill.

Some have wondered whether the judicial warrant requirement in the bill would pose a threat to the national security. No administration witness has suggested that it would, despite pointed and recurring questions on the issue, both in the open and closed session; however, they indicated that there may be risks in any new system of controlling intelligence activities. These can be risks of impeding or barring needed intelligence collection or risks of disclosure associated with controls on the activities. These risks, however, are inherent in any new control of intelligence activities and do not necessarily become greater because the controls are legislative, rather than executive, in origin or because judges are involved. Current Executive controls pursuant to

E.O. 12036, for example, substantially increase both type of risks over the situation that prevailed five or ten years ago. As to whether needed intelligence collection will be frustrated by this bill or its warrant requirement, Director of Central Intelligence, Stansfield Turner, testified:

> I cannot say that any proper or necessary government purposes will be frustrated by these statutes, or that vital intelligence information having such value as to justify electronic surveillance as a method of collection will be lost.

Moreover, since his testimony, the committee has made a number of amendments to the bill to assure that this is the case. No means of collection are barred by the bill, and the circumstances justifying collection are fully responsive to the intelligence agencies' need as they have been expressed to this committee.

As to risks of unauthorized disclosures, or "leaks," there is a "'rule" in intelligence that all other things being equal, the more persons who know of a secret, the more likely that it will be disclosed. Because judges will be involved in the approval process, as they have not been before, some have feared that the bill will be expanding the number of persons with knowledge of surveillances, thereby making "leaks" more likely. There are two answers to this. First, under the bill all other things are not equal, so even an increase in numbers of persons with knowledge, does not mean that "leaks" are more likely. One need only read the newspapers to realize that a primary cause of "leaks" is the uncertainty as to the legality and propriety of various intelligence activities. By eliminating that uncertainty with respect to foreign intelligence electronic surveillances, this bill will go a long way to stemming "leaks." Second, it is not even clear that this bill will increase the number of persons with knowledge of surveillances. Certain aspects of the bill, even where the warrant requirement is applicable, will result in substantially less paperwork within the executive branch, making possible a decrease in the number of persons with knowledge of the surveillances. Also, the bill, by its provisions dealing with subsequent challenges to the legality of surveillances, is likely to result in decreased numbers of persons to whom information concerning surveillances will be disclosed.

The fact that two successive administrations have supported a bill with a judicial warrant should be indicative of the fact that the bill and its warrant requirement do not threaten our national security or unnecessarily increase the risks to intelligence collection. Indeed, knowledgeable officials in the intelligence agencies have earnestly suggested to the committee that this bill will further our national security by facilitating the electronic surveillance necessary for foreign intelligence purposes.

Finally some witnesses before the Subcommittee on Legislation noted that this bill would generally not apply to surveillances overseas and expressed their concern about this area. The committee has explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillances. This is not to say that overseas surveillance should not likewise be subject to legislative authorization and

restriction, but the problems and circumstances of overseas surveillance demand separate treatment, and this bill, dealing with the area where most abuses have occurred, should not be delayed pending the development of that separate legislation. The committee notes the administration's commitment to the development of a separate bill governing overseas surveillances and expects to work closely with the administration on that bill.

Section-by-Section Analysis

Title I of the Foreign Intelligence Surveillance Act contains the substantive provisions governing the conduct of electronic surveillance for foreign intelligence purposes. Title II of the act contains certain amendments to chapter 119 of title 18, United States Code, governing the interception of wire and oral communications for law enforcement purposes, title III of the act contains the effective date and implementing provisions of the act.

As introduced, H.R. 7308 would have amended title 18 (Crimes and Criminal Procedure), United States Code, by creating a new chapter following chapter 119 which deals with law enforcement electronic surveillance. In the committee's view, the placement of title I in title 18 would be misleading. Nothing in title I relates to law enforcement procedures, and the one provision creating a criminal offense for intentional violations of the other provisions is pendent to the other provisions. Placing title I in title 18 would wrongly suggest either that the bill's procedures deal with law enforcement or that the thrust of the bill is to create a Federal crime. Because the bill instead establishes authorities and procedures dealing with the collection of foreign intelligence, the committee believes that its proper placement would be in title 50 (War and National Defense), United States Code. Title 50 has traditionally been the title in which laws relating to this Nation's intelligence activities have been placed, for example, the National Security Act of 1947 and the CIA Act of 1949.

This change from the bill as introduced, however, is not intended to affect in any way the jurisdiction of congressional committees with respect to electronic surveillance for foreign intelligence purposes. Rather, the purpose of the change is solely to allow the placement of title I in that portion of the United States Code which most directly relates to its subject matter.

Section 101

This section contains all the definitions of terms used in the bill. Because most of the substantive aspects of the bill derive from the definition of particular terms, this section is critical to the bill as a whole.

(*a*) "*Foreign power*"

Subsection (a) defines "foreign power" in six separate ways. These definitions are crucial because surveillances may only be targeted against foreign powers or agents of foreign powers.

It is expected that certain of the defined "foreign powers" will be found in the United States and targeted directly; others are not likely to be found in the United States but are included in the definition more to enable certain persons who are their agents, and who may be in the United States, to be targeted as "agents of a foreign power,"

as defined. As will appear below, the six categories well may overlap, and an entity may well be found to be a "foreign power" under more than one category. This is not improper. These categories are intended to be all-encompassing, and clear lines cannot always be drawn between different descriptions of the types of entities which justify targeting electronic surveillance. The six categories are:

(1) "A foreign government or any component thereof, whether or not recognized by the United States." This category would include foreign embassies and consulates and similar "official" foreign government establishments that are located in the United States.

(2) "A faction of a foreign nation or nations, not substantially composed of United States persons." 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. An example of such a faction might be the PLO, the Eritrean Liberation Front, or similar organizations. Specifically excluded from this category is any faction of a foreign nation or nations which is substantially composed of permanent resident aliens or citizens of the United States. The word "substantially" means a significant proportion, but it may be less than a majority.

(3) "An entity, which is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments." This category is specifically delineated in order to treat entities of this type in the same manner as the government they serve by including them within those "official" foreign powers subject to surveillance under a less stringent standard. That standard permits less information to be given to the judge, allows surveillance to be continued for a longer period of time, and in certain cases allows surveillance without a judicial warrant. Only entities "openly acknowledged" by a foreign government to be both directed and controlled by it are subject to this less strict standard.

Those entities which are clearly arms of a government or governments meet this definition. This category would include, for example, a legitimate commercial establishment which is directed and controlled by a foreign government. Such a legitimate commercial establishment might be a foreign government's airline, even though it was incorporated in the United States. Also included in this definition would be international organizations of states such as the Organization of Petroleum Exporting Countries or the Organization for African Unity. Where such organizations are involved, it is not necessary to show that one or two countries control the organization. Rather it is sufficient to show that the organization is made up of governmental entites which collectively direct and control the organization.

It is recognized that this type of foreign power includes corporations or organizations present in the United States which may have many United States citizens as employees

or even officers. Nevertheless, this fact does not detract from the fact that the organization acts as an arm of a foreign government or governments and as such may engage in activities directly affecting our national interests or security. In such circumstances a surveillance targeted against such an entity should focus on the activities of the organization, not its employees or members who are United States citizens, unless the activities of such employees or members directly relate to the activities of the organization. The minimization procedures required by section 101(h) will ensure that the surveillance is so focused and will ensure that the surveillance is not used for the purpose of gathering information concerning United States citizens which is not necessary to a legitimate foreign intelligence purpose. A focus on individual employees could be justified only by obtaining a separate court order for them as individuals.

A law firm, public relations firm, or other legitimate concern that merely represents a foreign government or its interests does not mean it is an entity in this category. The question whether a group, commercial enterprise, or organization comes within the scope of this definition is one for the court to answer on the basis of a probable cause standard.

(4) "A group engaged in international terrorism or activities in preparation therefor." The term "international terrorism" is a defined term, see section 101(c), and includes within it a criminal standard. A group under this category must be engaged in the activities described in section 101(c) or be in preparation therefor. Such groups would include Black September, the Red Army Faction, the Red Brigades, and the Japanese Red Army. It would not include groups engaged in terrorism of a purely domestic nature, which if surveillance is in order, should be subjected to surveillance under chapter 119 of title 18. Nevertheless, the citizenship of the terrorist group or its members while relevant to the determination of whether it is a "foreign power", is not determinative. As introduced, H.R. 7308 required that the group be "foreign-based," but in the world of international terrorism a group often does not have a particular "base," or if it does, it may be nearly impossible to discern. Perhaps more importantly, where its base is located is often irrelevant to the foreign intelligence interest or concern with respect to the group. While luckily the United States has heretofore been spared from the worst cases of international terrorism, a lack of intelligence concerning it may, as other countries crack down, present the United States as an inviting target. Even at this time, there are domestically based international terrorist groups, which have engaged in acts overseas which have resulted in deaths. Therefore, the committee has changed this definition from a "foreign-based" group engaged in undefined activities to a group engaged in criminal terrorist activities, which are international in scope or manner of execution, see section 101(c).

Generally, such groups will not be targeted in the United States as "foreign powers," if only because such a group is not likely to maintain an official presence here. Rather, members of the group may be in the United States either singly or in bunches, and they will be targeted as "agents of a foreign power," to wit, agents of a group engaged in international terrorism.

(5) "A foreign-based political organization, not substantially composed of United States persons." This category would include foreign political parties. In some countries, both totalitarian and parliamentary, ruling parties effectively control the government. Thus, information concerning the activities and intentions of these parties can directly relate to the activities and intentions of their government. Moreover, the intentions and positions of minorty parties can also be of great importance to this nation because, although minorities, they may affect the course of their government or they may come to power, in which case it would be important to have prior knowledge of their positions and intentions. Finally, this category is not limited to political parties; there are other foreign political organizations which exercise or have potential political power in a foreign country or internationally. Because it can be important to this nation to have intelligence concerning any organization which exercises or has potential political power in a foreign country or internationally targeting such organizations can be proper. On the other hand, where a political organization is domestically based or is substantially composed of U.S. persons and does not otherwise fall within the other definitions of "foreign power" or "agent of a foreign power," the gathering of political information concerning that organization by electronic surveillance—even though desired or even important to this Government—is improper and raises grave First Amendment questions. This definition 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.

(6) "An entity, which is directed and controlled by a foreign government or governments." This category is similar to category (3) above, except that the entity need not be openly acknowledged to be directed and controlled by a foreign government or governments. Such an entity must be acting as an arm of the government with respect to activities that are of foreign intelligence or counterintelligence significance. An example would be an entity which appears to be a legitimate commercial establishment, but which is being utilized by a foreign government as a cover for espionage activities. The concerns set forth with respect to openly controlled entities apply to this category as well. There is an added danger that electronic surveillance of a covertly controlled entity, substantially composed of U.S. persons, would potentially offer a means for evading the requirements for surveillance of indi-

vidual U.S. persons. Therefore, it is important to emphasize that the judge must find probable cause that the entity is both "directed" and "controlled" by a foreign government or governments. Merely following the directions of a foreign government which wants a group to lobby or speak out publicly on behalf of the government's interests, is not in itself sufficient to place the group in this category. While direction and control are separate elements to be established, the same evidence can demonstrate both.

Again, a law firm, public relations firm, etc. that merely represents a foreign mean government or its interests does not mean it is an entity in this category. An entity which ses its own interests as parallel to those of a foreign government and acts accordingly is not by this directed and controlled by that foreign government. It is only when the foreign government or its agents influence the entity to the extent that the entity yields its independent judgments that an entity becomes directed and controlled by a foreign government. In particular cases, obviously, it may be difficult to discern the actual direction and control, and, of course, circumstantial evidence may suffice in establishing probable cause, but no entity which purports to be a U.S. person should be considered directed and controlled by a foreign government *solely* on the basis that its activities are consistent with the desires of a foreign government.

(b) "*Agent of a foreign power*"

(1) *Non-resident aliens in the United States.*—There are two separable categories of the definition "agent of a foreign power." The first cannot be applied to United States citizens and permanent resident aliens; it is, therefore, limited to aliens in the United States who are tourists, visiting businessmen, exchange visitors, foreign seamen, diplomatic and consular personnel, illegal aliens, etc.

It is the view of the Department of Justice, with which the committee agrees, that most of the persons in this category are protected by the fourth amendment when they are in the United States. By requiring a judicial warrant issued on the basis of statutory criteria, such persons' fourth amendment protections have been increased from their status under current operating procedures of the executive branch. On the other hand, the protections afforded such persons are not as great as those afforded United States persons. The standard for targeting nonresident aliens does not have a criminal standard; there is no requirement to minimize the acquisition, retention, and dissemination of information with respect to such persons; no judge reviews the executive certification when such persons are targeted; and certain forms of electronic collection of communications would not require a warrant at all, because of the definition of electronic surveillance, see section 101(f)(1), where they would if a United States person was targeted. Some have questioned whether it is constitutional to treat nonresident aliens differently from United

States citizens in this context, either because the nonresident aliens' fourth amendment rights are violated or because to deny them protections afforded U.S. citizens denies them equal protection under the laws. The committee is convinced, however, that the protections afforded nonresident aliens in the bill fully satisfy the Constitution.

The basic test under the fourth amendment is that a search be reasonable. Reasonableness itself is determined by weighing the Government's legitimate need for the information sought against the invasion of privacy the search entails. The findings of probable cause required to be made by the judge as to nonresident aliens directly relate to the likelihood of obtaining foreign intelligence information from electronic surveillance of them. Such information by definition must directly and and substantially relate to important foreign policy or national security concerns, and high Executive officials must certify that the purpose of the surveillance is to obtain such information. On the other hand, Congress has plenary authority over the admission of aliens to the United States and can impose reasonable conditions to entry. Given the likelihood, which this committee has found, of obtaining foreign intelligence information from electronic surveillance of those nonresident aliens within the definition of "agent of a foreign power," this limitation of their privacy is in the committee's view reasonable under the fourth amendment.

As to the "equal protection" question, the committee notes that the Supreme Court has held that where there are compelling considerations of national security, alienage distinctions are constitutional.[21] Those distinctions must, however, be reasonable in light of the domonstrated need and not be overly broad. With respect to those non-resident aliens who fit within the two categories of agents of foreign powers in section 101(b)(1), that need has been demonstrated to this committee in testimony before it, primarily in closed session, as well as in public documents. Indeed, the committee has amended the provisions of H.R. 7308, as introduced, to tailor more specifically these categories in light of the demonstrated need.

Subsection (b)(1)(A) includes in its definition of "agent of a foreign power" those persons, who are not U.S. persons, who act in the United States as officers, members, or employees of a foreign power. As introduced, H.R. 7308 did not include non-U.S. persons who act as "members" of a foreign power in the United States. It was pointed out, however, that some "foreign powers," as defined, would not likely have "officers" or "employees." This would especially be true of groups engaged in international terrorism. Moreover, certain "foreign powers," as defined, would have "members" of more intelligence importance than mere employees. This could be espe-

[21] See, e.g. *Hampton* v. *Mow Sun Wong*, 426 U.S. 88, 116 (1976).

cially true of some foreign political parties. The committee finds ample evidence that non-resident aliens who act in the United States as officers, members, or employees of a foreign power are likely sources of foreign intelligence or counter-intelligence information. The definition excludes persons who serve as officers or employees or are members of a foreign power in their home country, but do not act in that capacity in the United States. The reference to employees of a foreign power is meant to include those persons who have a normal employee-employer relationship. It is not intended to encompass such foreign visitors are professors, lecturers, exchange students, performers or athletes, even if they are receiving remuneration or expenses from their home government in such capacity. The term "member" means an active, knowing member of the group or organization which is a foreign power. It does not include mere sympathizers, fellow-travelers, or persons who may have merely attended meetings of the group or organization. On the other hand, if a person has received terrorist training from a group engaged in international terrorism or clandestine intelligence training from a foreign organization, this would be substantial evidence that he was a member of such an entity. Subsection (b) (1) (B) defines an agent of a foreign power as a person who is not a U.S. person and who—

"Acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities."

This provision is substantially changed from H.R. 7308, as introduced. The change was made in response to comments voiced both by the FBI and some civil liberties groups. The FBI felt that the need in H.R. 7308, as introduced, to show that a foreign visitor was in fact engaged in clandestine intelligence activities was too restrictive in that surveillance was necessary with respect to certain foreign visitors, as to whom it could be shown with a high degree of probability that they would engage in clandestine intelligence activities, before sufficient information could be established showing they were so engaged. As a practical matter, less intrusive techniques may not enable the Government to obtain sufficient information about persons visiting the United States for only a limited time and who do not have a history of activities in the United States to show that they are indeed engaged in clandestine intelligence activities.

On the other hand, some civil liberties groups voiced concern over the fact that under H.R. 7308, as introduced, a non-criminal standard, relying on an undefined term—"clandestine intelligence activities", was being used as a basis for targeting

foreign visitors from any nation. In response, these groups suggested that the provision be narrowed only to apply to foreign visitors acting on behalf of certain foreign powers as to which it could be shown systematically engaged in clandestine intelligence activities threatening the security of the United States.

In light of these two legitimate concerns the committee has adopted the current provision which does not require a showing that the individual foreign visitor is himself currently engaged in clandestine intelligence activities, but rather that the circumstances of his presence here indicate that he may engage in such activities which are contrary to this nation's interests. In addition, it must be shown that he is acting for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States which are contrary to the interests of the United States. It is intended that the Government show that the foreign power has demonstrated some pattern or practice of engaging in clandestine intelligence activities in the United States contrary to the interests of the United States.

The phrase, "acts for or on behalf of a foreign power," is here intended to require the Government to show a nexus between the individual and the foreign power that suggests that the person is likely to do the bidding of the foreign power. For example, visitors from totalitarian countries present in the United States under the auspices, sponsorship, or direction of their government would satisfy this standard.

The term "interests" refers to important concerns or long-term goals of the United States, including interests embodied in law. It might be said that any country which engages in clandestine intelligence activities in the U.S. *ipso facto* acts contrary to this Nation's interests. This is clearly not intended here.

Once the requisite facts with regard to the foreign power are established, the question is whether the circumstances of the person's presence in the United States indicate that the person may engage in clandestine intelligence activities for that foreign power contrary to the interests of the United States. The answer to this question will vary according to what is known about the intelligence operations of the particular foreign power. Among the factors that might be taken into account are whether the foreign visitor engages in activities with respect to which there is evidence that other visitors who engage in similar activities are officers, agents, or acting on behalf of the intelligence service of that foreign power. If the Government can show from experience that a particular foreign power uses a certain class of visitors to this country for carrying out secret intelligence assignments, this too would indicate that a visitor in this class may engage in clandestine intelligence activities.

The standard "may engage in such activities" means that surveillance can be conducted to anticipate clandestine intelli-

gence activities by such persons, rather than waiting until after they have taken place. The additional standards for aiding or abetting, and conspiracy, require probable cause that the foreign visitor is knowingly assisting persons who are already engaged in clandestine intelligence activities. The "knowingly" requirements are the same as in the aiding or abetting and conspiracy standard for U.S. persons. See section 101(b)(2)(D), *infra*.

This provision does not treat nationals of certain countries differently from others solely on the basis of their nationality. Instead, coverage of the nationals of other countries depends on the activities of the governments of those countries and whether the individual is acting on behalf of the government.

The term "clandestine intelligence activities" is intended to have the same meaning as in section 101(b)(2)(A) and (B) described *infra*.

(2) "*Any person*".—Under H.R. 7308, as introduced, there were four categories under the definition of "agent of a foreign power" which could apply to any person, e.g., a United States citizen. One of these categories did not require any showing of possible criminal activity. Another category was a conspiracy provision which, because it referred to the non-criminal standard, could have authorized surveillance of one "conspiring" with someone not engaged in criminal activity. While the witnesses before the Subcommittee on Legislation acknowledged that the activity described in the non-criminal standard was "tantamount to a crime," there was apprehension by some that the bill was authorizing electronic surveillance of United States citizens without any explicit showing of criminal activity.

New language was, therefore, developed by the Administration and congressional leaders, with the participation of interested outside parties, including the ACLU.

This Committee welcomed the spirit behind this compromise because it requires that whenever a United States person is to be the target of a surveillance there must be showing that his activities at least may involve a violation of law.

As a matter of principle, this Committee agrees that no United States citizen in the United States should be targeted for electronic surveillance by his government absent some showing that he at least may violate the laws of our society. A citizen in the United States should be able to know that his government cannot invade his privacy with the most intrusive techniques if he conducts himself lawfully.

On the other hand, this committee recognizes full well that the surveillance under this bill are not primarily for the purpose of gathering evidence of a crime. They are to obtain foreign intelligence information, which when it concerns United States persons must be necessary to important national concerns. Combatting the espionage and covert actions of other nations in this country is an extremely important national concern. Prosecution is one way, but only one way and not always the best way, to combat such activities. "Doubling" an agent or feeding him false or useless information are other ways. Monitoring him to discover other spies, their tradecraft and equipment can be

vitally useful. Prosecution, while disabling one known agent, may only mean that the foreign power replaces him with one whom it may take years to find or who may never be found.

The committee also recognizes that strict standards applicable to the most intrusive techniques of investigation may not be appropriate for other less intrusive techniques. In the course of considering charter legislation for intelligence agencies, the proper standards for other forms of investigation will have to be addressed, but the decision here with respect to electronic surveillance does not mean the same standard must be applied to all techniques.

(A) Clandestine Intelligence Gathering

Paragraph (2)(A) allows surveliance of any person who is knowingly engaged in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States.

The first aspect of this definition is that the person is engaging in such acts "knowingly." This does not mean that he must know, or that the Government must show that he knows, that he may be violating a Federal criminal law. It does mean that he must know that he is engaging in clandestine intelligence gathering activities and that he knows that he is doing so on behalf of a foreign power. It is often difficult to prove what a person knows and what he does not know. The committee intends that circumstantial evidence should be sufficient to show the requisite knowledge. If, for example, a person is transmitting classified defense secrets to the military attache of a foreign embassy, this should be sufficient to show that he knows that he is acting for or on behalf of a foreign power. Similarly, if a person has received training in or equipment for espionage, for example a microdot camera or disguised radio device, this too should be sufficient to show that he knows what he is doing. While this, and the other provisions under paragraph (2), are not intended to reach one who in fact is ignorant as to the nature of what he is doing, the knowing requirement is not intended to force the Government to disprove his ignorance when a person engaged in such activities would reasonably suspect that he was acting for or on behalf of a foreign power.

Next, the person must be "engaged" in the proscribed activities. Unlike the standard for foreign visitors, the fact that he "may engage" in these activities some time in the future is not sufficient. For example, if evidence shows that a person has recently engaged in the activities, this would normally suffice to show probable cause that he is "engaged" in such activities now.

On the other hand, evidence that a person engaged in the proscribed activities six months or longer ago might well, depending on the circumstances and other evidence, be sufficient to show probable cause that he is still engaged in the activities. For instance, evidence that a U.S. person was for years a spy for a power currently hostile to the United States, but who had dropped out of sight for a few years, would probably be sufficient to show "probable cause" that he was, having now reappeared, continuing to engage in the clandestine intelligence activities.

Probably the most critical term in this provision is "clandestine intelligence gathering activities." It is anticipated that most clandestine intelligence gathering activities will constitute a violation of the various federal criminal laws aimed at espionage either directly or by failure to register, see e.g., 18 U.S.C. §§ 792–799, 951; 42 U.S.C. §§ 2272–2278b; and 50 U.S.C. § 855. The term "clandestine intelligence gathering activities" is intended to have the same meaning as the word espionage in normal parlance, rather than as a legal term denoting a particular criminal offense. The term also includes those activities directly supportive of espionage such as maintaining a "safehouse," servicing "letter drops," running an "accommodation address," laundering funds, recruiting new agents, infiltrating or exfiltrating agents under cover, creating false documents for an agent's "cover," or utilizing a radio to receive or transmit instructions or information by "burst transmission." "Clandestine intelligence gathering activities" are intended to be activities which no reasonable person would engage in without knowing that society would not condone it. As the words indicate, the activities must be "clandestine," that is, efforts have been taken to conceal the activities.

This does not necessarily mean that the information gathered by the agent must itself be secret or nonpublic, although this would usually be the case. It is possible that a spy may be tasked to obtain information which is technically available to the public, but which a foreign power would not like it known that it was seeking. If the spy, for instance, used false identification or ruse to obtain the information and then delivered the information by means of a microdot hidden in a magazine left at a "dead drop," both the means by which he gathered and the means by which he transmitted the information would be "clandestine," even though the information itself might not be secret. It can be proper for the Government to monitor such a person, even if the information he is collecting at that moment is not secret, because his activities identify him as a spy. On the one hand, having done his job successfully he may be given a new assignment to collect secret information. On the other hand, by monitoring his contacts in this enterprise, their equipment, and modus operandi, the Government can learn valuable information concerning the tactics, capabilities, and personnel of the foreign intelligence service.

Obviously, gathering classified defense information, information about intelligence sources and methods, and classified diplomatic information qualifies as clandestine intelligence gathering activities if it is done in a clandestine manner. In addition, the committee is aware that foreign powers also target their intelligence apparatus against American technology and trade secrets, economic developments, political information, and even personal information for purposes of blackmail or other coercion. The gathering of any such information may be within the term "clandestine intelligence gathering activities."

As noted above, "clandestine intelligence gathering activities" are intended to be conduct of the nature associated with spies and espionage in its generic sense, but the term is supposed to be flexible with respect to what is being gathered because the intelligence priorities and requirements differ between nations and over time, and this bill is intended to allow surveillance of different foreign powers' intelligence activities well into the future.

It is possible, although unlikely, that certain groups of Americans might indeed come close to using espionage techniques for otherwise lawful purposes. Thus, the provision requires as a separate element of proof that the person be engaged in clandestine intelligence gathering activities "for or on behalf of a foreign power." This means that the Government will have to show probable cause to believe that the person is not only engaged in clandestine intelligence gathering activities, but also that those activities are for or on behalf of a foreign power. Thus, if all that can be shown is that a person is stealing defense secrets and using a "dead drop" to pass them on, the Government will have to show more, that is, probable cause to believe that he is doing this for a foreign power.

Similarly, the fact that a person gathers information and transmits it to a foreign power by itself does not satisfy the standard of this definition. Americans for personal or commercial reasons may legitimately gather information for foreign powers, as indeed registered lobbyists often do, but their activity, if legitimate, does not utilize the tradecraft of espionage.[22] Thus, there seems little likelihood that a person would be engaged in clandestine intelligence gathering activities for or on behalf of a foreign power and not in fact be engaged in reprehensible conduct of substantial concern to this Nation's security.

As an added safeguard, however, the Government must also show that there is probable cause to believe that the person is engaged in activity that at least may violate the Federal criminal law. As noted above, it is expected that most persons under this definition would be likely to violate laws directed against espionage. In addition, there are other laws which might be violated, for example, 18 U.S.C. section 2514 which proscribes the interstate transportation of stolen property; and 50 U.S.C. section 2021–2032, the Export Administration Act.

The words "may involve" as used in this subparagraph are not intended to encompass individuals whose activities clearly do not violate Federal law. They are intended to encompass individuals engaged in clandestine intelligence gathering activities which may, as an integral part of those activities, involve a violation of Federal law. They cover the situation where the Government cannot establish probable cause that the foreign agent's activities involve a specific criminal act, but where there are sufficient specific and articulable facts to indicate that a crime may be involved.

This "may involve" standard replaces the noncriminal standard which appeared in H.R. 7308, as introduced. Both the former provision, and the "may involve" standard, address the same problem. The committee has concluded that it is necessary in order to permit the Government to investigate adequately in cases such as those where Federal agents have witnessed "meets" or "drops" between a foreign intelligence officer and a citizen who might have access to highly classified or 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 that a crime was involved or what specific crime was being committed. Nevertheless, the

[22] The Committee does not intend that "clandestine intelligence gathering activities" must necessarily include the use of espionage tradecraft, but its use is significant.

committee believes that the circumstances might be such as to indicate that the activity may involve a crime. The crime involved might be one of several violations depending, for example, upon the nature of the information being gathered.

In applying this standard, the judge is expected to take all the known relevant circumstances into account—for example, who the person is, where he is employed, whether he has access to classified or other sensitive information, the nature of the clandestine meetings or other clandestine activity, the method of transmission, and whether there are any other likely innocent explanations for the behavior. It is intended, 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 there is probable cause to believe the activity may involve a Federal criminal violation.

The term "may involve" not only requires less information regarding the crime involved, but also permits electronic surviellance at some point prior to the time when a crime sought to be prevented, as for example, the transfer of classified documents, actually occurs. There need not be a current or imminent violation if there is probable cause that criminal acts may be committed. The committee recognizes that an argument can be made that a person could be surveilled for an inordinate period of time. That is clearly not the intention. 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 "may involve." Surveillance cannot be justified unless there is probable cause to believe that the person is engaged in such activities, even though the relationship of those activities to a specific violation of law may be more uncertain or likely to occur in the future.

It should be clear from the foregoing, but for the sake of explicitness the committee wishes to make perfectly clear, that surveillance would not be authorized under this, or any other definition of agent of a foreign power against an American reporter merely because he gathers information for publication in a newspaper, even if the information was classified by the Government. Nor would it be authorized against a Government employee or former employee who reveals secrets to a reporter or in a book for the purpose of informing the American people. This definition would not authorize surveillance of ethnic Americans who lawfully gather political information and perhaps even lawfully share it with the foreign government of their national origin. It obviously would not apply to lawful activities to lobby, influence, or inform Members of Congress or the administration to take certain positions with respect to foreign or domestic concerns. Nor would it apply to lawful gathering of information preparatory to such lawful activities.

In the case of an organization whose leaders are engaged in clandestine intelligence gathering activities, such activity cannot be attributed to every member of the group. There must be probable cause that a particular member is himself engaged in such activity before electronic surveillance targeted against him may be authorized under this subparagraph.

In short. for a person to be an agent of a foreign power under this definition he must be knowingly engaged in clandestine intelligence activities, like espionage, for or on behalf of a foreign power, and those activities must be such that they at least "may involve" a violation of Federal criminal law.

A particularly difficult problem may arise where a person is "turned" or "doubled;" that is, having started as an agent for a foreign power, he is persuaded instead to work for this Government. The standard under this paragraph requires that a person knowingly engage in activities for or on behalf of a foreign power. If the person is in fact working for this Government and not for the foreign power, this standard is obviously not met and he could not be surveilled under this paragraph. Often, however, there may be substantial doubt whether he is acting under this Government's control or under the control of a foreign power. It may well be unclear which side is deceiving which. The committee recognizes that the fact that a supposedly "doubled" agent indeed does carry out his assignments and instructions from this Government does not mean that he has stopped carrying out his assignments and instructions from the foreign power contrary to this Government's interest. It is not the committee's intent that a surveillance, once authorized, need be discontinued when the agent may have been "doubled". Rather, it is the committee's intent that, until such time as the "doubled" agent is trusted enough to seek his consent to surveillance, he may continue to be surveilled as acting for or on behalf of a foreign power.

(B) "Other clandestine intelligence activities"

Paragraph (2)(B) defines agent of a foreign power as a person who pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in "any other clandestine intelligence activities" for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States.

The term "any other clandestine intelligence activities" is intended to refer to covert actions by intelligence services of foreign powers. Not only do foreign powers engage in spying in the United States to obtain information, they also engage in activities which are intended to harm the Nation's security by affecting the course of our Government, the course of public opinion, or the activities of individuals. Such activities may include political action (recruiting, bribery or influencing of public officials to act in favor of the foreign power), disguised propaganda (including the planting of false or misleading articles or stories), and harassment, intimidation, or even assassination of individuals who oppose the foreign power. Such activity can undermine our democratic institutions as well as directly threaten the peace and safety of our citizens.

On the other hand, there may often be a narrow line between covert action and lawful activities undertaken by Americans in the exercise of their first amendment rights. Because of this, whereas H.R. 7308, as introduced, did not distinguish between "clandestine intelligence gathering activities" and "any other clandestine intelligence activities," a

stricter standard has been created—stricter than that applicable to "clandestine intelligence gathering activities" and stricter than that applicable in H.R. 7308, as introduced—which must be satisfied before a person may be targeted as an agent of a foreign power under this definition.

First, the person must be shown to be acting "pursuant to the direction of an intelligence service or network of a foreign power." No such showing is required for any of the other definitions of agent of a foreign power. Americans may well communicate with non-intelligence personnel from the government of a country about which they have an interest to gain information or to engage in efforts on behalf of that country, but this is not covert action and it is not intended to be covered by this definition.

Second, the activities engaged in must presently involve or be about to involve a violation of Federal criminal law. Again, this is a higher standard than is found in the other definitions, where the activities "may" involve a violation of law. In this area where there is close line between protected First Amendment activity and the activity giving rise to surveillance, it is most important that where surveillance does occur the activity be such that it involves or is about to involve a violation of a Federal criminal statute.

There are a number of crimes that might be involved in covert actions, for example, bribery of public officials, campaign law violations, foreign agent registration requirements, denial of civil rights, et cetera. It is important to note, however, that the fact of a criminal violation does not establish or even necessarily suggest, that a person is engaged in "any other clandestine intelligence activity." Americans through ignorance or inadvertence may well technically violate campaign law requirements or foreign agent registration requirements, and such violations do not even justify surveillance for law enforcement purposes, see 18 U.S.C. section 2516. Under this definition it is necessary to show separately from the criminal violation that the facts support a probable cause to believe that the person is, pursuant to the direction of an intelligence service or network of a foreign power, knowingly engaged in any other clandestine intelligence activities for or on behalf of such foreign power.

The intent of this provision is to enable surveillance of those hard-core agents who are witting as to what they are doing and who are intentionally carrying out the bidding of a foreign power's intelligence service to engage in covert action in the United States.

(C) Sabotage or Terrorism

Paragraph (2)(C) allows surveillance of any person, including a U.S. person, who knowingly engages in sabotage or international terrorism, or activities which are in preparation therefor, for or on behalf of a foreign power. The terms "sabotage" and "international terrorism" are defined separately and require a showing of criminal activity. Again, in no event is mere sympathy for, identity of interest with, or vocal support for the goals of a foreign group, even a foreign-based terrorist group, sufficient to justify surveillance under this subparagraph. The term "activities which are in preparation" for sabotage or

international terrorism is intended to encompass activities supportive of acts of serious violence—for example, purchase or surreptitious importation into United States of explosives, planning for assassinations or financing of or training for such activities. Of course, other activities supportive of terrorist acts could in other circumstances likewise satisfy this standard. The circumstances must be such as would lead a reasonable man to conclude that there is probable cause to believe the person is knowingly engaged in activities which are in preparation for sabotage or terrorism.

The term "preparation" does not require evidence of preparation for one specific terrorist act, because the definition of "international terrorism" speaks of "activities which involve violent acts" and means a range of acts, not just a single act. Here, the term "preparation" acquires its meaning in the context of the special definition of "international terrorism," which could reasonably be interpreted to cover, for example, providing the personnel, training, funding, or other means for the commission of acts of terrorism, rather than one particular bombing. The committee has also adopted the "preparation" provision in order to permit electronic surveillance at some point before the danger sought to be prevented—for example, a kidnaping, bombing, or hijacking—actually occurs. This standard is in no way intended to dilute the requirement of knowledge, or the requisite connection with a "foreign power" as defined in 1801(a).

Concern has been expressed from some quarters that this subparagraph could permit surveillance solely on the basis of information that someone might commit acts of international terrorism or sabotage in the distant future. This is clearly not the intent of the committee. There must be a showing that the person is currently engaged in activities which are in preparation for the commission of such acts.

The "preparation" standard would allow surveillance where the Government cannot establish probable cause that an individual has already knowingly engaged in sabotage or terrorism, but where there are sufficient specific and articulable facts to indicate that the individual's activities are in preparation for sabotage or international terrorism. The judge is expected to take all the known circumstances into account. The circumstances must be such as would lead a reasonable man to conclude that there is probable cause to believe the person is knowingly engaged in activities which are in preparation for sabotage or terrorism.

It should be noted that the "preparation" standard only need apply where there is insufficient evidence to show that the person is in fact a terrorist. Where the Government can show that the person is a known international terrorist, like the notorious "Carlos," or that the person has been engaging in international terrorism for or on behalf of a group engaged in international terrorism, there is no need to show that the person is in the act of preparing for further terrorist acts. One might wonder why the Government would not immediately arrest such persons. In some cases they may not have violated U.S. law, even though they may have murdered hundreds of persons abroad. In other cases it may be more fruitful in terms of combatting international terrorism to monitor the activities of such persons in the United States to identify otherwise unknown terrorists here, their

international support structure, and the location of their weapons or explosives. If a person who has engaged in international terrorism visits the United States or resides in the United States, the Government should be able to utilize electronic surveillance to monitor his activities, whether or not there is evidence to show he is presently planning some particular violent act.

Finally, any person targeted for surveillance under this paragraph must be shown to have a knowing connection with the "foreign power" for whom he is working. In the case of international terrorism, it is anticipated that in most cases this connection will be shown to exist with a group engaged in international terrorism. The case may arise where a U.S. person is acting for or on behalf of such a group that is substantially composed of U.S. persons. In such a case, the judge must examine the circumstances carefully in order to determine whether the organization is "a group engaged in international terrorism," as defined, and not a purely domestic group engaged in domestic terrorism. In the latter cases, the Government must rely on the domestic law enforcement surveillance procedures of title III of the Omnibus Crime Control Act of 1968, contained in chapter 119, of title 18, United States Code, if it wishes to engage in surveillance.

(D) Aiding, Abetting and Conspiracy

Paragraph (2)(D) allows surveillance of any person, including a U.S. person, who knowingly aids or abets any person in the conduct of activities described in subparagraphs (2)(A)–(C) above, or knowingly conspires with any person to engage in such activities. The knowledge requirement is applicable to both the status of the person being aided by the proposed subject of the surveillance and the nature of the activity being promoted. This standard requires the Government to establish probable cause that the prospective target knows both that the person with whom he is conspiring or whom he is aiding or abetting is engaged in the described activities as an agent of a foreign power and that his own conduct is assisting or furthering such activities. The innocent dupe who unwittingly aids a foreign intelligence officer cannot be targeted under this provision. In the case of a person alleged to be knowingly aiding or abetting those engaged in international terrorism on behalf of a foreign power, such a person might be assisting a group 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 the group's lawful activity.

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, Dr. King could not have been found to be one who knowingly aids or abets a foreign agent.

As was noted above, however, the "knowing" requirement can be satisfied by circumstantial evidence, and there is no requirement for the Government to disprove lack of knowledge where the circumstances were such that a reasonable man would know what he was doing.

(c) *International terrorism*

Subsection (c) defines the term "international terrorism" by requiring three separate aspects of activities to be shown. The first aspect describes the nature of the acts involved in the activity; the activities must involve "violent acts or acts dangerous to human life" which are or may be a violation of either State or Federal law, or which, if committed in the United States, would likely violate either State or Federal law. The committee intends that terrorists and saboteurs acting for foreign powers should be subject to surveillance under this bill when they are in the United States, even if the target of their violent acts has been within a foreign country and therefore outside actual Federal or State jurisdiction. This departure from a strict criminal standard is justified by the international responsibility of governments to prevent their territory from being used as a base for launching terrorist attacks against other countries as well as to aid in the apprehension of those who commit such crimes of violence.

We demand that other countries live up to this responsibility and it is important that in our legislation we demonstrate a will to do so ourselves.

The second aspect of this definition relates to the purpose to which the activities are directed. The purpose of the terrorist activities must be either the intimidation of the civilian population, the intimidation of national leaders in order to force a significant change in government policy, or the affecting of government conduct by assassination or kidnapping. Examples of activities which in and of themselves would meet these requirements would be: the detonation of bombs in a metropolitan area, the kidnapping of a high-ranking government official, 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 country, the deliberate assassination of persons to strike fear into others to deter them from exercising their rights or the destruction of vital governmental facilities. Of course other violent acts might also satisfy these requirements if the requisite purpose is demonstrated.

The third aspect of this definition relates to the requirement that the terrorist activities be international or foreign in scope. In H.R. 7308, as introduced, this aspect was not present in the definition of terrorism.

The committee has amended the original language of the bill to require that the terrorist activities must occur totally outside the United States or otherwise be international in character. Thus, if a member of the Baader-Meinhof Group or the Japanese Red Army, who has engaged in terrorist acts abroad, comes to the United States, he or she may be immediately placed under surveillance. If the activities have not occurred totally outside the United States, then it must be shown that the activities transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum. Remembering that this is a definition of "international terrorism," there must be a substantial international character with respect to these considerations. The fact that an airplane is hijacked while flying over Canada between Alaska and Chicago does not by itself make the activity international terrorism. A domestic terrorist group which explodes a bomb in the international arrivals area of a U.S. airport does not by this alone become engaged in international terrorism. However, if a domestic group kidnaps foreign officials in the United States or abroad to affect the conduct of that foreign government this would constitute international terrorism. If a domestic group travels abroad and places a bomb in a foreign airplane, this too would be international terrorism. Finally, if a domestic terrorist group receives direction or substantial support from a foreign government or foreign terrorist group, its terrorist activities made possible by that support or conducted in response to that direction could be international terrorism. It is important, however, to recognize that this substantial support or direction must already have been established before surveillance could be authorized. This definition does not allow for electronic surveillance of Americans merely to determine if they are receiving foreign support or direction. Moreover, support is not intended to include moral or vocal support. It must be material, technical, training, or other substantive support, and the support must be of the acivities involving the terrorist acts, not just general support to a group which may engage in both terrorist activities as well as other lawful activities. Direction means direction and does not mean suggestions.

Activities parallel to or consistent with the desires of a foreign power do not by themselves satisfy the requirement that the foreign power is directing the domestic group.

Finally, the fact that particular members of a domestic group engage in international terrorism does not mean that all members of that group are similarly engaged.

(*d*) *Sabotage*

Subsection (d) defines sabotage as activities which involve or may involve crimes under chapter 105 of title 18, United States Code, if conducted against the United States. By its terms, chapter 105 makes criminal only acts of sabotage against U.S. Government facilities. This bill expands the definition of sabotage to include similar acts when committed against a State or another nation's facilities and materials relating to defense. Thus, sabotage directed against state and local police facilities and equipment, or against the defense facilities of foreign nations, would constitute sabotage under this definition. Of course, electronic surveillance under this chapter could be undertaken only if such sabotage was knowingly conducted for or on behalf of a "foreign power" as defined and the information sought constituted foreign intelligence as defined. Where persons have knowingly engaged in sabotage of State or foreign facilities for or on behalf of a foreign power, such persons should be subjected to foreign intelligence electronic surveillance in this country even in the absence of probable cause to believe that they will engage in sabotage against Federal facilities.

(*e*) *Foreign intelligence information*

As introduced, H.R. 7308 defined foreign intelligence information as information which was "necessary" for the United States to protect against foreign attack, terrorism, sabotage, or clandestine intelligence activities or was "essential" to the national defense or security or to the successful conduct of this nation's foreign affairs. The committee found two faults with this formulation. First, the distinction between "essential" and "necessary" seemed strained and more likely to confuse than to clarify the issues. Second, the committee agreed with the testimony of the Defense Department that the "necessary"/"essential" standard was too strict where the information did not concern U.S. persons.

The primary thrust of this bill is to protect Americans both from improper activities by our intelligence agencies as well as from hostile acts by foreign powers and their agents. Any information which relates to these general security and foreign relations concerns can help protect Americans and their interests from hostile activities of foreign powers. Where this information does not concern U.S. persons, the countervailing privacy considerations militating against seeking such information through electronic surveillance are outweighed by the need for the information. Therefore, the committee has adopted a definition of foreign intelligence information which includes any information relating to these broad security or foreign relations concerns, so long as the information does not concern U.S. persons. Where U.S. persons are involved, the definition is much stricter; it requires that the information be "necessary" to these security or foreign relations concerns.

Where the term "necessary" is used, the committee intends to require more than a showing that the information would be useful or convenient. The committee intends to require a showing that the information is both important and required. The use of this standard is intended to mandate that a significant need be demonstrated by those seeking the surveillance. For example, it is often contended that a counterintelligence officer or intelligence analyst, if not the policymaker himself, must have every possible bit of information about a subject because it might provide 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.

Subparagraph (e)(1)(A) of this subsection defines foreign intelligence information as information which relates to, and if concerning a U.S. person, is necessary to, the ability of the United States to protect against actual or potential attack or other grave hostile acts of a

foreign power or its agents. This category is intended to encompass information which relates to foreign military capabilities and intentions, as well as 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 subparagraph which is keyed to actual or potential attack.

Thus, only grave types of hostile acts would be envisioned as falling within this provision.

Subparagraph (e)(1)(B) of this subsection includes information which relates to, and if concerning a U.S. person, is necessary to, the ability of the United States to protect against sabotage or terrorism by 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 against the type of foreign power defined in section 101(a)(4), or against the type of foreign agent defined in section 101(b)(2)(C).

Subparagraph (e)(1)(C) of this subsection includes information which relates to, and if concerning a U.S. person, is necessary to, the ability of the United States to protect against the clandestine intelligence activities by an intelligence service or network of a foreign power or by a foreign agent. This subparagraph encompasses classic counterintelligence information.

This subsection is not intended to encompass information sought about political activity by U.S. citizens allegedly "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 been the basis for improper investigations of citizens in the past and is not intended to be a permissible avenue of "foreign intelligence" collection under this subparagraph. Nor does this subparagraph include efforts to prevent "newsleaks" or to prevent publication of such leaked information in the American press, unless there is reason to believe that such leaking or publication is itself being done by an agent of a foreign intelligence service to harm the national security.

Information about a U.S. person's private affairs is not intended to be included in the meaning of "foreign intelligence information" unless it may relate to his activities on behalf of a foreign power. For example, the Government should not seek purely personal information about a U.S. citizen or permanent resident alien, who is a suspected spy, merely to learn something that would be "compromising." This restriction might not be applicable to agents of foreign powers as defined in section 101(b)(1), because compromising information about their private lives may itself be foreign intelligence information.

It should be noted that under paragraph (e)(1) there is no requirement that the attack, grave hostile act, sabotage, terrorism, or clandestine intelligence activities be directed against the United States in order for information to constitute "foreign intelligence information", as defined. Obviously, armed attacks and similar grave hostile acts against any nation in this interdependent world more often than not directly affect the security and foreign relations of all countries. War in the Mideast or in the Horn of Africa, for example, inevitably involves this nation's security and foreign relations. Sabotage and international terrorism also, even if confined to one foreign country, may indeed affect the interests and security of the United States. The kidnaping of a high official of an allied nation can affect the course of government and security of that nation, thereby affecting this nation's security and foreign relations. Finally, clandestine intelligence activities of one nation directed against another can easily affect this nation. This occurred in West Germany where Soviet spies in the German Defense Ministry compromised NATO secrets, which included American secrets. It can also occur when other nations engage in clandestine intelligence activities against one another in the United States.

Finally, the term "foreign intelligence information," especially as defined in subparagraphs (e)(1)(B) and (e)(1)(C), can include evidence of certain crimes relating to sabotage, international terrorism, or clandestine intelligence activities. With respect to information concerning U.S. persons, foreign intelligence information includes information necessary to protect against clandestine intelligence activities of foreign powers or their agents. Information about a spy's espionage activities obviously is within this definition, and it is most likely at the same time evidence of criminal activities. How this information may be used "to protect" against clandestine intelligence activities is not prescribed by the definition of foreign intelligence information, although, of course, how it is used may be affected by minimization procedures, *see* section 101(h), *infra*. And no information acquired pursuant to this bill could be used for other than lawful purposes, *see* section 106(a). Obviously, use of "foreign intelligence information" as evidence in a criminal trial is one way the Government can lawfully protect against clandestine intelligence activities, sabotage, and international terrorism. The bill, therefore, explicitly recognizes that information which is evidence of crimes involving clandestine intelligence activities, sabotage, and international terrorism can be sought, retained, and used pursuant to this bill.

Paragraph (e)(2) of this subsection includes information which relates to, and if concerning a U.S. person, is necessary to, (A) the national defense or the security of the Nation or (B) the conduct of the foreign affairs of the United States. This also requires that the information sought involve information with respect to foreign powers or territories, and would therefore not include information solely about the views or planned statements or activities of Members of Congress, executive branch officials, or private citizens concerning the foreign affairs or national defense of the United States.

It is anticipated that the types of "foreign intelligence information" defined in subparagraph (e)(1)(A) and (e)(2) (A) and (B) will be the types most often sought when an electronic surveillance is instituted against a foreign power as defined in section 101(a)(1)–(3) and (5), or against most foreign agents as defined in section 101 (b)(1)(A).

Consideration was given to a standard of "important," rather than "relates to," for information concerning foreign powers and foreign persons collected to serve these more nebulous national defense, national security, and foreign affairs interests. However, the committee did not wish to impose a standard under which responsible executive

branch officials could not honestly certify that entirely proper and appropriate activities were conducted to produce "foreign intelligence information," as defined here. Certain other limitations are present. The information must pertain to a foreign power or foreign territory; and thus it cannot simply be information about a citizen of a foreign country who is visiting the United States unless the information would contribute to meeting intelligence requirements with respect to a foreign power or territory. With these limitations, the committee believes that the adoption of a "relates to" standard would not authorize improper treatment. In this regard, the committee fully intends that the vigorous exercise of its oversight authority will provide another valuable check.

(*f*) *Electronic surveillance*

Subsection (f) defines electronic surveillance to include four separate types of activities.

(1) *Intentionally targeting.*—Paragraph (1) protects U.S. persons who are located in the United States from being targeted in their domestic or *international* communications without a court order no matter where the surveillance is being carried out. The paragraph covers the acquisition of the contents of a wire or radio communication of a U.S. person by intentionally targeting that particular, known U.S. person, provided that the person is located within the United States. Thus, for example, any watchlisting activities of the National Security Agency [24] conducted in the future, directed against the international communications of particular U.S. persons who are in the United States, would require a court order under this provision.

Only acquisition of the contents of those wire or radio communications made with a reasonable expectation of privacy where a warrant would be required for law enforcement purposes is covered by paragraph (1). It is the committee's intent that acquisition of the contents of a wire communication, without the consent of any party thereto, would clearly be included.

The term "intentionally targeting" a particular, known U.S. person who is in the United States includes the deliberate use of a surveillance device to monitor a specific channel of communication which would not be surveilled but for the purpose of acquiring information about a party who is a particular, named U.S. person located within the United States.[25] It also includes the deliberate use of surveillance techniques which can monitor numerous channels of communication among numerous parties, where the techniques are designed to select out from among those communications the communications to which a particular U.S. person located in the United States is a party, and where the communications are selected either by name or by other information which would identify the particular person and would select out his communications.

This paragraph does not apply to the acquisition of the contents of international or foreign communications, where the contents are not

[24] See Church committee hearings, vol. 5, esp. pp. 5–24; Church Committee Report, book II, pp. 58–60, 108 and 308–311, and book III, pp. 733–783.

[25] This would include wiretapping a foreign official when the intent and purpose of the wire tap is to hear the conversations of a particular U.S. person with that foreign official, if the foreign official would not otherwise have been wiretapped for different purposes. Such a case has occurred in the past. See "Church Committee Report," book II, p. 228.

acquired by intentionally targeting a particular known U.S. person who is in the United States. Therefore, this bill does not afford protections to U.S. persons who are abroad, nor does it regulate the acquisition of the contents of international communications of U.S. persons who are in the United States, where the contents are acquired unintentionally. The committee does not believe that this bill is the appropriate vehicle for addressing this area. The standards and procedures for overseas surveillance may have to be different than those provided in this bill for electronic surveillance within the United States or targeted against U.S. persons who are in the United States.

The fact that this bill does not bring the overseas surveillance activities of the U.S. intelligence community within its purview, however, should not be viewed as congressional authorization of such activities as they affect the privacy interests of Americans. The committee merely recognizes at this point that such overseas surveillance activities are not covered by this bill. In any case, the requirements of the fourth amendment would, of course, continue to apply to this type of communications intelligence activity.[26] *Cf.*, *Berlin Democratic Club* v. *Rumsfeld*, 410 F. Supp. 144 (DDC 1976).

(2) *Wire communications.*—Paragraph (2) includes 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 when such acquisition occurs in the United States. As this subdefinition makes clear, one party to the wire communication may be outside the United States 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.

The surveillance covered by paragraph (2) is not limited to the acquisition of the oral or verbal contents of a wire communication. It includes the acquisition of any other contents of the communication, for example, where computerized data is transmitted by wire. Therefore, it includes any form of "pen register" or "touch-tone decoder" device which is used to acquire, from the contents of a wire communication, the identities or locations of the parties to the communication. Examination of telephone billing records in documentary form is not covered. The committee is concerned about the need to protect the privacy of such confidential records of the provision of telecommunications services, but does not believe that this bill is the appropriate measure in which to do so.

(3) *Radio communications.*—Paragraph (3) includes the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of a totally domestic radio communication, without the consent of any party thereto, made with a reasonable expectation of privacy and under circumstances where a warrant would be required for law enforcement purposes, where both the sender and all intended recipients are located within the United States. This part of the def-

[26] The Committee notes with approval that electronic surveillance of American citizens while abroad has been limited in part both by the President's Executive Order applicable to the U.S. intelligence community and by procedures approved by the Attorney General. See Executive Order 12036, Jan. 24, 1978; testimony of Attorney General Edward H. Levi, Church committee hearings, vol. 2, p. 66 ff.

inition would reach not only the acquisition of communications made wholly by radio but also the acquisition of communications which are carried in part by wire and in part by radio, where the radio transmitted portion of those communications are intercepted. The territorial limits of this subdefinition are not dependent on the point of acquisition, as is the case with subdefinition (2), but on the locations of the sender and intended recipients of the communication. Thus, the acquisition of radio communications outside the territorial limits of the United States would be covered if all of the parties were located within the United States. Only acquisition of those domestic radio communications made with a reasonable expectation of privacy where a warrant would be required for law enforcement purposes would be included in the term "electronic surveillance." This would exclude for example, commercial broadcasts, as well as ham radio and citizen band radio broadcasts (cf. 47 U.S.C. section 605); *United States* v. *Hall* 488 F.2d 193 (9th Cir. 1973).

It is the committee's intent that the intentional acquisition of the contents of a communication being transmitted by common carrier radio microwave, without the consent of any party thereto and where all parties to the communication are located in the United States, would clearly be included here. The intentional acquisition of such contents is not limited to the intentional acquisition of oral or verbal contents. It includes the intentional acquisition of any other comments, as described with respect to paragraph (2).

Only "intentional" acquisitions of private domestic radio communications are within this subdefinition because, by their very nature, radio transmissions may be intercepted anywhere in the world, even though the sender and all intended recipients are in the United States. Thus, intelligence collection may be targeted against foreign or international communications but accidentally and unintentionally acquire the contents of communications intended to be totally domestic. As amended by this committee, the bill would require the destruction of such contents in almost all circumstances. See Sec. 106(j), *infra*.

(4) *Other monitoring.*—Paragraph (4) brings within the definition of "electronic surveillance" the installation or use of an electronic, mechanical, or other surveillance device for monitoring in the United States under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. 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 required in the ordinary criminal context. *United States* v. *Holmes*, 537 F.2d 227 (5th Cir. 1976). 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 the statutory procedures. It is not meant to include, however, the acquisition of those international radio transmissions which are not acquired by targeting a particular U.S. person in the United States. 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.[27] But two persons in a public park, far from any stranger, should not reasonably anticipate that their conversations could be overhead from afar through a directional microphone, and so would retain their right of privacy.

The definition of "electronic surveillance" applying to wire communications has an explicit exception where any party has consented to the interception. This is intended to be consistent with existing 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.[28] Such consent need not be explicit, but whether consent may be inferred in a particular case will depend on the facts and circumstances. The other definitions of "electronic surveillance" require that the acquisition of information be under circumstances in which a person has a constitutionally protected right of privacy. There may be no such right in situations where the acquisition is consented to by at least one party to the communication or 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 informant may have no justifiable expectation that the informant will not repeat, record, or even transmit by a miniature transmitter what the person voluntarily tells the informant.[29]

The committee does not intend the term "surveillance device" as used in paragraph (4) to include devices which are used incidentally as part of a physical search, or the opening of mail, but which do not constitute a device for monitoring. Lock picks, still cameras, and similar devices can be used to acquire information, or to assist in the acquisition of information, by means of physical search. So-called chamfering devices can be used to open mail. This bill does not bring these activities within its purview. Although it may be desirable to develop legislative controls over physical search techniques, the committee has concluded that these practices are sufficiently different from electronic surveillance so as to require separate consideration by the Congress. The fact that the bill does not cover physical searches for intelligence purposes should not be viewed as congressional authorization for such activities. In any case, any requirements of the fourth amendment would, of course, continue to apply to this type of activity.[30]

The provisions that "a warrant would be required for law enforcement purposes" do not mean that a court must previously have required a warrant for the particular type of surveillance activity carried out under paragraph (1), (3), or (4). The techniques involved may not have come before a court for a determination as to whether a warrant is required. Nevertheless, the surveillance activity is in-

---

[27] *Air Pollution Variance Board* v. *Western Alfalfa Corp.*, 416 U.S. 861 (1974). The Committee's intent is not to have this definition apply to overhead surveillance.

[28] *Lopez* v. *United States*, 373 U.S. 427 (1963); *Rathbun* v. *United States*, 355 U.S. 197 (1957).

[29] *United States* v. *White*, 401 U.S. 745 (1971); but see the dissenting opinion of Mr. Justice Harlan for a contrary view.

[30] It should be noted that Executive Order 12036, Jan. 24, 1978, places limits on physical searches and the opening of mail.

tended to be covered if a warrant would be required for law enforcement purposes, as determined on the basis of an assessment of the similarity with other surveillance activities which the courts have ruled upon, and the reasonableness of the expectation of privacy that a U.S. person would have with respect to such activity.

In response to questions from the committee, the Department of Justice opined that foreign governments—and in some circumstances their diplomatic agents have no fourth amendment rights under the Constitution, *see* footnote 34, infra. Whether the Department of Justice is correct in its opinion, on an issue which has never been addressed by any court, the coverage of the definition of "electronic surveillance" is not intended—by the use of the words "a warrant would be required for law enforcement purposes"—to exclude surveillances merely because they are targeted against an entity or person not entitled to protection under the fourth amendment. Rather, the phrase is intended to exclude only those surveillances which would not require a warrant even if a U.S. citizen were the target. The committee expects that, if an agency wishes to use a new surveillance technique, it will seek a ruling from the Attorney General as to whether the technique requires a court order. The intelligence committees should be advised of such rulings.

Law enforcement officials may, if they wish, continue to obtain an ordinary search warrant or chapter 119 court order if the facts and circumstances justify it.

(*g*) "*Attorney General*"

Subsection (g) defines "Attorney General" to mean the Attorney General of the United States, the Acting Attorney General, or the Deputy Attorney General. H.R. 7308, as introduced, permitted a specially designated Assistant Attorney General to approve such applications. The administration saw a need to lessen the administrative burden on the Attorney General which would be perpetuated even after this bill has established the safeguards of a court order procedure.

Relying on the assurance of Attorney General Bell in his testimony before the Senate Judiciary Committee on S. 1566 that he would personally continue to approve applications under the bill until standards of review have been well established, the committee has adopted a modified version of the Administration's proposal. It provides authority for the Attorney General (or the Acting Attorney General) or the Deputy Attorney General—rather than a specially designated Assistant Attorney General—to approve applications for an electronic surveillance order under this chapter. The Deputy Attorney General is appropriate because, as the second-ranking official in the Justice Department, he would most often be the Acting Attorney General in the Attorney General's absence.

(*h*) "*Minimization procedures*"

The minimization procedures of the bill provide vital safeguards because they regulate the acquisition, retention, and dissemination of information about U.S. persons, including persons who are not the authorized targets of surveillance. For example, an entirely innocent American might use a telephone that is tapped to target someone else.

Or an American might talk on the phone to a foreign official who is under surveillance for purposes unrelated to the particular conversation. The procedures also protect Americans who are not parties to a communication, but who are referred to in the communication; such information has in the past been disseminated for improper purposes.

Paragraph (1) of subsection (h) defines "minimization procedures" as specific procedures reasonably designed to minimize the acquisition, retention, and dissemination of any non-publicly available information concerning unconsenting U.S. persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

The definition begins by stating that the minimization procedures must be specific procedures. This is intended to demonstrate that the definition is not itself a statement of the minimization procedures but rather a general statement of principle which will be given content by the specific procedures which will govern the actual surveillances. It is also intended to suggest that the actual procedures be as specific as practicable in light of the technique of the surveillance and its purposes.

The definition then states that the procedures must be "reasonably designed in light of the purpose and technique of the particular surveillance." It is recognized that minimization procedures may have to differ depending on the technique of the surveillance. For instance, minimization with respect to essentially physical surveillance techniques such as closed-circuit TV and "beepers" would not be comparable to minimization of intercepted communications.

In addition, in many cases it may not be possible for technical reasons to avoid acquiring all information. In these situations, the reasonable design of the procedures must emphasize the minimization of retention and dissemination. The procedures may also differ given the purpose of the surveillance. Where the purpose of a surveillance is to obtain foreign intelligence information as defined in section 101(e)(2), the procedures may be able to be very strict with respect to what may be retained or disseminated concerning U.S. persons, and on what basis. This is reflected in paragraph (2) of this subsection, *see infra*. Where the purpose of a surveillance is to gather foreign intelligence information as defined in section 101(e)(1)(B) or (C), however, some flexibility must be provided with respect to the retention of information concerning U.S. persons. Innocuous-sounding conversations may in fact be signals of important activity; information on its face innocent when analyzed or considered with other information may become critical. Nevertheless, strict controls to preclude improper dissemination may be found necessary.

The definition of minimization speaks in terms of acquisition, retention and dissemination.

By minimizing acquisition, the committee envisions, for example, that in a given case, where A is the target of a wiretap, after determining that A's wife is not engaged with him in clandestine intelligence activities, the interception of her calls on the tapped phone, to which A was not a party, probably ought to be discontinued as soon as it is realized that she rather than A was the party. Or, where a switchboard line is tapped but only one person in the organization is

the target, the interception should probably be discontinued where the target is not a party. In other cases, however, it may not be possible or reasonable to avoid acquiring all conversations. It is recognized that given the nature of intelligence gathering, minimizing acquisition should not be as strict as under chapter 119 of title 18 with respect to law enforcement surveillances. For this very reason, while chapter 119 does not require minimizing retention and dissemination, this bill does.

By minimizing retention, the committee intends that information acquired, which is not necessary for obtaining producing, or disseminating foreign intelligence information, be destroyed where feasible. For example, after determining that A's wife is not engaged with her husband in clandestine intelligence activities, her communications, acquired and retained in order to make this determination, might be able to be destroyed. Indeed, even A's communications which are clearly not relevant to his clandestine intelligence activities could be destroyed. In certain cases destruction might take place almost immediately, while in other cases the information might be retained for a reasonable period in order to determine whether it did indeed relate to one of the approved purposes. Procedures governing minimization—particularly how long information should be retained and how it should be destroyed once it is deemed irrelevant—are normally approved by the court and subject to judicial supervision.

The committee recognizes that it may not be feasible to cut and paste files or erase part of tapes where some information is relevant and some is not. Therefore, minimizing retention can also include other measures designed to limit retention of such irrelevant material to an essentially non-usable form.

Under dissemination requirements information being held to determine its usefulness should not be disseminated until that determination was made (or would only if disseminated to those who could determine its usefulness). Even with respect to information needed for an approved purpose, dissemination should be restricted to those officials with a need for such information. And, again, the judge, in approving the minimization procedures, could require specific restrictions on the retrieval of such information.

There are a number of means and techniques which the minimization procedures may require to achieve the purpose set out in the definition. These may include, where appropriate, but are not limited to:

(A) destruction of unnecessary information acquired;

(B) provisions with respect to what may be filed and on what basis, what may be retrieved and on what basis, and what may be disseminated, to whom, and on what basis;

(C) provision for the deletion of the identity of United States persons where not necessary to assess the importance or understand the information;

(D) provisions relating to the proper authority in particular cases to approve the retention or dissemination of the identity of United States persons;

(E) provisions relating to internal review of the minimization process; and

(F) provisions relating to adequate accounting of information concerning United States persons used or disseminated.

Minimization, however, is not required with respect to all information which may be acquired by electronic surveillance. First, publicly available information need not be minimized. By publicly available, the Committee means information which in fact is generally available to the public. Such information can include generally published information or information in the public record which is generally available to the public, e.g., statements of incorporation on file in state offices. Also included would be trade names such as a Xerox copier, a Boeing 747, etc. Second, where a person has consented to waive minimization with respect to the acquisition, retention, or dissemination of information about him through electronic surveillance, no minimization is required. The committee intends that this consent be *explicit* and *informed*. A general authorization to obtain information about him, such as may be made by a person seeking Government employment, is not sufficient. As here used, consent to waive minimization must be specific with respect to the acquisition, retention, and dissemination of information concerning the person acquired by electronic surveillance. There is not, however, any requirement that the person know the time, manner, purpose, or target of any particular surveillance. It is expected that this allowance will be used rarely and then with respect to high ranking Government officials. Obviously, refusal to consent should not in any sense be held against a person.

Finally, only information concerning a United States person need be minimized. This includes both communications to which a United States person is a party as well as communications to which he is not a party but which mention him. The Supreme Court has held that persons have no constitutionally protected right of privacy with respect to what others say about them. See *Alderman* v. *United States*, 394 U.S. 165 (1968). Nevertheless, the use of such information in the past has been abused, and the Executive Branch in its own porcedures has demonstrated that it can minimize the retention and dissemination of such information consistent with legitimate foreign intelligence needs. Recognizing the less substantial privacy interest in such information, however, the "reasonably designed" procedures may take account of the differences between information in which persons have a constitutionally protected interest and that in which they do not. Therefore, more flexibility in the procedures may be afforded with respect to information concerning U.S. persons obtained from communications of others. Of course, information concerning U.S. persons may come from other than communications which are intercepted, yet under circumstances where their privacy is invaded; in such situations the person subjected to the surveillance either as the target or incidentally has had his privacy interests invaded and minimization procedures are required.

Because minimization is only required with respect to information concerning U.S. persons, where communications are encoded or otherwise not processed, so that the contents of the communication are unknown, there is no requirement to minimize the acquisition, retention, or dissemination of such communications until their contents are known. Nevertheless, the minimization procedures can be structured to apply to other agencies of the Government, so that if any agency different from the intercepting agency decodes or processes the com-

munication, it could be required to minimize the retention and dissemination of information therein concerning U.S. persons.

It is recognized that parties to communications are unlikely to state at the outset that they are or are not U.S. persons. Intelligence officers and analysts therefore must use their judgment as to when the procedures apply. While not suggesting that the procedures require the following, as a general rule, the committee believes that persons in the United States might be presumed to be U.S. persons unless there is some reason to believe otherwise, as may well be the case depending on certain possible targets. Intelligence personnel might indicate in reports or logs that persons are not U.S. persons, therefore making self-explanatory why the information is not minimized.

The committee does not intend or expect, however, that interceptors will delete or destroy possibly meaningful information merely because there is a question whether a person is a U.S. person.

The definition states that the minimization procedures must minimize the acquisition, retention, and dissemination of information subject to minimization "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information".

"Foreign intelligence information" is, of course, a defined term, and with respect to information concerning U.S. persons, it must be "necessary" to the listed security and foreign relations purposes. However, the definition of "minimization procedures" does not state that only "foreign intelligence information" can be acquired, retained, or disseminated. The committee recognizes full well that bits and pieces of information, which taken separately could not possibly be considered "necessary," may together or over time take on significance and become "necessary." Nothing in this definition is intended to forbid the retention or even limited dissemination of such bits and pieces before their full significance becomes apparent.

An example would be where the Government is wiretapping a known spy, who is a U.S. person. It is "necessary" to identify anyone working with him in his network, feeding him his information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence. Where after a reasonable period of time, which may in fact be an extended period of time, there is no reason to believe such persons are involved in the clandestine intelligence activities, there should be some effort, for example, either to destroy the information concerning such persons, or seal the file so that it is not normally avialable, or to make the file not retrievable by the name of the innocent person. It is recognized that the failure to gather further incriminating information concerning the contacts or acquaintances of the spy does not necessarily mean they are in fact innocent—instead, they may merely be very sophisticated and well-versed in their espionage tradecraft. Therefore, for an extended period it may be necessary to have information concerning such acquaintances re-

trievable, for a tap on another spy may indicate the same acquaintance, which may justify more intensive scrutiny of him, which then may result in breaking his cover.[31]

It is disconcerting to some that mere association with an alleged spy may be enough to cast suspicion on a person such that his innocence must be established. It seems contradictory to one of our basic tenets that a person is presumed innocent in the eyes of the law until proven guilty. However, in intelligence as in law enforcement, leads must be followed. Especially in counterintelligence cases where often trained professional foreign intelligence personnel are involved, a lead which initially ends in a "dry hole" can hardly be considered a dead issue, although it may be temporarily shelved to divert limited resources to other leads. Therefore, this committee intends that a significant degree of latitude be given in counterintelligence and counterterrorism cases with respect to the retention of information and the dissemination of information between and among counterintelligence components of the Government.

On the other hand, given this degree of latitude the committee believes it imperative that with respect to information concerning U.S. persons which is retained as necessary for counterintelligence or counterterrorism purposes, rigorous and strict controls be placed on the retrieval of such identifiable information and its dissemination or use for purposes other than counterintelligence or counterterrorism.

In this regard, the committee believes it is important to note two points governing dissemination. First, the procedures should recognize that use within an agency may be subject to minimization.

Many agencies have widely disparate functions themselves, or are subordinate elements of departments which have functions totally unrelated to intelligence. It is the intent of the committee that use within an agency is potentially subject to minimization. While restrictions on use within an agency need not necessarily be the same as the restrictions on interagency dissemination, it is clear that some controls on intraagency use are appropriate.

Second, some might consider that any derogatory information concerning a person holding a security clearance or concerning a person who in the future might be considered for a security clearance would be information disseminable as being for "counterintelligence" purposes. This is not intended.

The latitude the committee intends to afford counterintelligence components with respect to retention and dissemination between them of information for counterintelligence and counterterrorism purposes is not designed or intended to allow the same latitude for general personnel security purposes.

Where the purpose of a surveillance is not counterintelligence or counterterrorism, there probably is not the same compelling need for latitude in the retention of information concerning U.S. persons. The committee is aware of classified procedures now in effect which minimize the acquisition, retention, and disclosure of information concern-

[31] It bears repeating that electronic surveillance could not be targeted against such acquaintances until it could be shown that they were in fact an agent of a foreign power, as defined.

ing U.S. persons in such cases and believes they are fully responsive to the definition in this subsection.

With respect to the unclassified dissemination procedures currently governing the FBI, the committee expects that they will be reviewed and appropriately modified in light of the requirements of this bill.

One of the results of minimizing retention and dissemination under this bill is that much information will be destroyed, retained in a non-identifiable manner, or sealed in a manner to prevent dissemination. This is a substantial change from the treatment of wiretap product under chapter 119 of title 18. There, section 2518(a) requires that all interceptions be recorded, if possible, and that the tapes not be edited or destroyed for 10 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 when criminal prosecutions are undertaken it is clear that the evidence is intact and has not been tampered with. Although there may be cases in which information acquired from a foreign intelligence surveillance will be used as evidence of a crime, these cases are expected to be relatively few in number, unlike chapter 119 interceptions, the very purposes of which is 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, the better practice is to allow the destruction of information that is not foreign intelligence information or evidence of criminal activity. This course will safeguard the privacy of individuals more effectively, insuring that irrelevant information will not be filed. The committee believes that existing criminal statutes relating to obstruction of justice will deter any efforts to tamper with evidence acquired under this chapter. Such destruction should occur, of course only pursuant to the minimization procedures.

Destruction insures that the information cannot be used to "taint" a civil or criminal proceeding; accordingly, there is no requirement to index, for purposes of 18 U.S.C. section 3504, information which is destroyed or otherwise not used or disseminated.

The definition of minimization procedures states that the Attorney General shall adopt appropriate procedures. In most cases, of course, these procedures will be reviewed and approved, modified, or disapproved by the judge approving the surveillance. In those cases where no warrant is required, where there is little or no likelihood that Americans will be intercepted, no judge will review the procedures, and it is important that it is the Attorney General, as the chief law enforcement officer, who ultimately approves them. It is expected that the procedures adopted by the Attorney General will have been thoroughly coordinated with the affected agencies in the executive branch.

The committee has learned in the course of its consideration of minimization procedures that in certain circumstances problems could be caused if different minimization procedures were to be imposed on different surveillances. In some cases, for instance, individuals responsible for minimizing might not even know which particular surveillance resulted in a particular piece of information. In other cases, it simply would be unreasonable to require an interceptor manning several different wiretaps to keep straight which procedures apply to which tap. Therefore, the committee wishes to express its intent that where these or other factors militate in favor of uniformity, to the maximum degree possible the minimization procedures be kept as uniform as possible. This does not mean, however, that judges should not fully scrutinize proposed minimization procedures just because the same procedures have been approved by another judge in another case. Not only might the earlier judge have overlooked something, but also it is critical to determine at the least that factors militating in favor of uniformity are not outweighed by other considerations. For instance, certain factors might favor uniformity in minimization procedures governing wiretaps of both an embassy and a foreign spy acting as a newspaper reporter, but the committee expects that the minimization procedures with respect to the latter would be more strict to assure that information unrelated to his spy activities was not misused. If the judge believes a modification is called for, he should require it. If the Government finds the change unacceptable, it may, of course, appeal the decision to the Special Court of Appeals, *see* section 103(b).

Paragraph (2) of the definition requires that all minimization procedures contain a requirement that any information acquired which is not foreign intelligence information as defined in section 101(e)(1) not be disseminated in a manner which identifies an individual United States person, without his consent, unless the identity is necessary to understand foreign intelligence information or to assess its importance. The purpose of this special dissemination standard is to protect individual United States persons from dissemination of information which identifies them in those areas where the Government's need for their identity is the least established and where abuses are most likely to occur. This special dissemination proviso is a safeguard against such abuses. Two exceptions to this prohibition on dissemination exist.

The first allows dissemination where a U.S. person's identity is "necessary to understand" foreign intelligence information. The person's identity must be needed to make the information fully intelligible. If the information can be understood without identifying the person, it should be disseminated that way. However, sometimes it might be difficult or impossible to make sense out of the information without a U.S. person's identity. One example would be the identity of a person who is the incumbent of an office of the executive branch of the U.S. Government having significant responsibility for the conduct of U.S. defense or foreign policy, such as the Secretary of State or the State Department country desk officer. The identities of such persons would frequently satisfy the "necessary to understand" requirement, especially when such person is referred to in the communications of foreign officials. This example does not mean, however, that all the conversations of a particular executive branch official with foreign officials who are under surveillance should be automatically or routinely reported to the U.S. official's superior without his knowledge or consent.

The second exception allows dissemination where a U.S. person's identity is necessary to "assess [the] importance" of foreign intelligence information. The word "importance" means important in terms of the interests set out in the definition of foreign intelligence infor-

mation. For example, if a foreign government is negotiating with an American business firm to purchase nuclear materials, it might be important to the national defense or security—in a military sense—or to the successful conduct of the Government's nonproliferation policy, to know the identity of the business firm involved. That might be the only way the State Department could determine whether a deal is likely to be made. On the other hand, the information may turn out not to be important. The question under the bill is whether the identity of the person or entity is needed to assess that importance.

Paragraph (3) of the definition relates to information which is evidence of a crime. In H.R. 7308, as introduced, no provision was made in the minimization procedures themselves for retaining or disseminating evidence of a crime. Instead, in another part of the bill, there was a general statement that the minimization procedures did not bar retention and dissemination of information which is evidence of a crime. The committee felt that this arrangement was slightly confusing and that it should be recognized in the definition of the minimization procedures and the procedures themselves that the procedures do not bar retention and dissemination of evidence of a crime. As noted above, *see* section 101 (e), evidence of certain crimes like espionage would itself constitute "foreign intelligence information," as defined, because it is necessary to protect against clandestine intelligence activities by foreign powers or their agents. Similarly, much information concerning international terrorism would likewise constitute evidence of crimes and also be "foreign intelligence information," as defined. This paragraph does not relate to information, even though it constitutes evidence of a crime, which is also needed by the United States in order to obtain, produce or disseminate foreign intelligence information. Rather this paragraph applies to evidence of crimes which otherwise would have to be minimized because it was not needed to obtain, produce, or disseminate foreign intelligence information. For example, in the course of a surveillance evidence of a serious crime totally unrelated to intelligence matters might be incidentally acquired. Such evidence should not be required to be destroyed. Where the information is not foreign intelligence information, however, retention and dissemination of such evidence is allowed only to prevent the crime or to enforce the criminal law. Thus, this paragraph is not a loophole by which the Government can generally keep and disseminate derogatory information about individuals which may be a technical violation of law, where there is no intent actually to enforce the criminal law. On the other hand, where the evidence also constitutes "foreign intelligence information," as defined, this paragraph does not apply, and the information may be disseminated and used for purposes other than enforcing the criminal law.

Paragraph (4) is responsive to the committee's amendment allowing certain surveillances of certain foreign powers to be conducted without judicial authorization. *See* section 102(a). As is expained *infra*, the reason for this amendment is the extreme sensitivity of these special surveillances weighed against the extreme unlikelihood of intercepting any U.S. person's communications even incidentally. Because, however, the balance against extending the number of persons with knowledge of these surveillances, even to a small number of judges, relies on the

fact that U.S. persons will not be intercepted, it is necessary that the minimization procedures contain an extremely tough provision with respect to U.S. person communications to assure that the nonwarrant procedure is not used in fact to intercept Americans. This paragraph requires the destruction of an intercepted communication to which a U.S. person is a party unless within 24 hours a court order is obtained where the judge is fully apprised as to the surveillance and where he approves the minimization procedures. An exception to this rule is provided only where the information may indicate death or serious bodily harm to any person.

(*i*) *U.S. person*

Section 101(i) defines a "United States person" to include a citizen of the United States, a permanent resident alien, an unincorporated association of which a substantial number of its members are citizens of the U.S. or permanent resident aliens, or a corporation incorporated in the United States. However, unincorporated associations or corporations which are "foreign powers," as defined in section 101(a) (1)–(3), cannot be "United States persons," no matter what their membership or place of incorporation.

The bill is designed to afford primary protection to "United States persons." Thus, minimization is only required with respect to information concerning U.S. persons; only when U.S. persons are targeted does a judge review the Executive certification, *see* section 105(a)(5); the definition of "foreign intelligence information" is much broader where non-U.S. persons are involved; and surveillance of international communications is generally only within the definition of "electronic surveillance" if a "United States person" is the target, *see* section 101(f)(1). Under H.R. 7308, as introduced, however, associations and corporations which would otherwise be within the definition of "United States person" and entitled to the consequent protections were excluded from the definition if they were within the definition of "foreign power." The committee has amended the definition of "United States person" so as to exclude associations or corporations, which would otherwise be United States persons, only if they are also within the first three subdefinitions of "foreign power," *see* section 101(a)(1)–(3).

The effect of this change is to treat as "United States persons" groups allegedly engaged in international terrorism, *see* section 101(a)(4), and entities allegedly covertly directed and controlled by a foreign government or governments, *see* section 101(a)(6), if they are substantially composed of U.S. citizens or permanent resident aliens or incorporated in the United States, and foreign-based political organizations if they are incorporated in the United States. This change does *not* in any way prohibit surveillance of such associations or corporations if they meet the definition of "foreign power." What it does is assure that the intentional surveillance of the international communications of such entities in the United States, by intentionally targeting them, will require a court under the bill and a judicial determination that the entity is in fact a "foreign power." Absent this change, intelligence agencies would be free to target the international communications of any entity *they* felt was a "foreign power;" there would be no requirement for minimization; and no judicial determination or review of anything—because the activity would not be regu-

lated by the bill at all. Such an exclusion from the bill would create potential for abuse, because large numbers of U.S. corporations or dissident groups could be targeted in their international communications without any judicial oversight and without any minimization of information concerning U.S. citizens, whether connected with the targeted entity or not.

This change in the definition of "United States person" also has an important effect where a U.S. corporation or an association substantially composed of Americans is targeted for surveillance under the bill as a "foreign power" as defined in section 101(a) (4)–(6). Under H.R. 7308, as introduced, a warrant would be required for surveillance of other than international communications, but the executive certification would only need to assert that the information sought "related to" broad national security or foreign relations concerns, and the judge would not be able to review that certification at all. This change would require in these circumstances that the executive certification assert that the information is "necessary" to the national security or foreign relations concerns, and would require that the judge review that certification on a "clearly erroneous" basis. This is critical where the target of a surveillance is "an entity directed and controlled by a foreign government or governments," see section 101(a)(6). Such an entity may be entirely composed of U.S. citizens; it may also be engaged in totally lawful and proper activities. The committee has been persuaded that there may be a legitimate need for surveillance of such an entity where it is directed and controlled by a foreign government or governments, but the committee feels that this non-criminal standard can only be supported so long as such entities, which are either incorporated in the United States or substantially composed of U.S. citizens or permanent resident aliens, are treated as United States persons. The added scrutiny that results from a certification that the information is "necessary" and judicial review of the certification is the minimum which the committee feels can justify such a broad targeting standard with respect to an entity composed of Americans or incorporated in the United States.

Finally, this change also mandates that information concerning entities which are incorporated in the U.S. or which are substantially composed of Americans be subject to minimization even if the entities also might be foreign powers, as defined in section 101(a)(4)–(6). Under H.R. 7308, as introduced, U.S. citizens and permanent resident aliens who might be members of such entities would be protected by minimization but the entities would not. Where a judge has approved the targeting of such an entity and reviewed the executive certification that the information sought is necessary, it is not expected that much minimization would be required as to the entity. For instance, if a group of Americans is a group engaged in international terrorism, it is expected that almost all information about the group would be "necessary" to the United States to protect against international terrorism. However, a domestic political group might be found by a judge to be covertly directed and controlled by a foreign government, and information concerning that direction and control might be found necessary to protect the United States against clandestine intelligence activities. But that entity might also engage in legitimate political activities not

relating to the foreign government's direction and control. In such a circumstance the committee believes minimization is both appropriate and important.

The committee does not believe the special protections afforded U.S. persons are appropriate where an association or corporation is a "foreign power" as defined in section 101(a)(1)–(3). The entities covered by these subdefinitions are not subject to much doubt. They are all "official" foreign powers more likely than not flying a foreign flag outside their door. Thus, there is little opportunity for error or abuse by intelligence agencies.

The term "unincorporated association" in the definition of "United States person" is meant to include any group, entity, or organization which is not incorporated under the laws of the United States or of any State. The term "members" here, as opposed to its use in section 101(b)(1)(A), is not intended, of course, to be limited to formal, card-carrying members. For instance, an unincorporated commercial establishment's employees would be members under this definition. The committee intends the reference to "a substantial number of members" to be equivalent to the term "substantially composed of" used in parts (2) and (5) of the definition of "foreign power." In both contexts the words "substantial" or "substantially" require that there be a significant proportion, but less than a majority. The judge is expected to take all the known circumstances into account in determining whether an association is a "United States person."

(j) United States

Section 101(j) defines the term "United States" when it is used in a geographic sense, see section 101(f). As defined, the United States includes all areas under the territorial sovereignty of the United States whether incorporated or not, e.g., Puerto Rico, Guam, the Virgin Islands, and American Samoa. The Trust Territory of the Pacific Islands is not, at this time, under the territorial sovereignty of the United States. It is, however, included in the term "United States" for purposes of this bill, so long as it is under the trusteeship of the United States. As trustee for the people of these islands, the United States has a duty to include those islands under the umbrella of the protections afforded the rest of the United States. Revelations of CIA electronic surveillance activities in Micronesia make such a duty all the more important. At such time as all or part of the Trust Territory enters into a Commonwealth relationship with the United States, it is intended that any such part be considered under the territorial sovereignty of the United States. If the trusteeship is ended with parts or all of the islands becoming independent, this bill would not apply to those parts.

The term "territorial sovereignty" in the definition does not include U.S. embassies, consulates, military or other U.S. flag vessels outside the United States, etc.; it does include land in the United States occupied by foreign embassies, consulates, missions, etc. Despite the fact that foreign missions are sometimes referred to as being "extraterritorial," all nations maintain territorial sovereignty over foreign missions and may expel, as persona non grata, persons therein and condemn the property by right of eminent domain. Military bases and areas under military occupation abroad (e.g. the United States sector

in West Berlin) are not under the territorial sovereignty of the United States.

In the bill terms such as "foreign-based" and "foreign territory" refer to places outside the "United States," as defined here.

(k) Aggrieved person

Section 101(k) defines the term "aggrieved person" as a person who has been the target of an electronic surveillance or any other person who, although not a target, has been incidentally subjected to electronic surveillance. As defined, the term is intended to be coextensive, but no broader than, those persons who have standing to raise claims under the Fourth Amendment with respect to electronic surveillance. See *Alderman* v. *United States*, 394 U.S. 316 (1968).

The term specifically does not include persons, not parties to a communication, who may be mentioned or talked about by others. The Supreme Court has specifically held in *Alderman* that such persons have no fourth amendment privacy right in communications about them which the Government may intercept. While under this bill minimization procedures require minimization of communications about U.S. persons, even though they are not parties to the communication, there is no intent to create a statutory right in such persons which they may enforce. Suppression of relevant criminal evidence and civil suit are particularly inappropriate tools to insure compliance with this part of minimization. Review by judges pursuant to section 105(d), Executive oversight and congressional oversight by the Senate and House Intelligence Committees are intended to be the exclusive means by which compliance with minimization procedures governing minimization of "mentions of" U.S. persons is to be monitored under this or any other law.

(l) Wire communication

Section 101(l) defines "wire communication" to mean any communication (whether oral, verbal, or otherwise) while it is being carried by a wire, cable, or other like connection furnished or operated by a communications common carrier. This definition of wire communication differs from the definition of the same term in chapter 119 of title 18, United States Code. There the term is defined to include any communication carried in whole or in part by a wire furnished by a common carrier. This has led to anomalous results such as where a woman listening to an ordinary FM radio has intercepted radio-telephone communications and thereby technically violated chapter 119. See *United States* v. *Hall*, 488 F. 2d 193 (9th Cir. 1973). Also, ordinary marine band communications, which do not have a reasonable expectation of privacy or require a warrant for law enforcement interception, can be "patched into" telephone systems, becoming a "wire communication" under chapter 119.

The definition here makes clear that communications are "wire communications" under the bill only while they are carried by a wire furnished or operated by a common carrier. The term "common carrier" means a U.S. common carrier and not a common carrier in a foreign country. Moreover, the word "furnished" means furnished in the ordinary course of the common carrier's provision of communications facilities. It does not refer to equipment sold outright to a

person. The effect of this is to require a tap on the wire, an induction coil or like device to acquire the communication from the wire furnished by the common carrier for the activity to be electronic surveillance under section 101(f)(2). Interception of microwave communications carried by common carriers, by intercepting the radio signal, is electronic surveillance under section 101(f)(3), not section 101(f)(2), involving acquisition of a radio communication, not a wire communication. A radio signal is not within the term, a "like connection," in this definition.

(m) Person

Section 101(m) defines "person" in the broadest sense possible. It is intended to make explicit that entities can be persons, where the term "person" is used. For example, while it is expected that most entities would be targeted under the "foreign power" standard (which cannot be applied to individuals), it is possible that entities could be targeted under certain of the "agent of a foreign power" standards, see section 101(b)(2)(A)–(D). Where it is intended that only natural persons are referred to, the term "individual" U.S. person or "individual" person is used.

(n) Contents

Section 101(n) defines the term "contents", when used with respect to any communication, in broad terms. Specifically, it includes any information concerning the identities of the parties or the existence, substance, purport, or meaning of a communication. This broad phrasing is meant to assure that the scope of the bill is sufficient to protect legitimate privacy interests. Inasmuch as three of the four subdefinitions of electronic surveillance, which in fact define the coverage of the bill, turn on the acquisition of "contents" it is necessary to assure that devices such as pen registers are included.

In a recent decision,[32] the Supreme Court suggested that a pen register did not acquire "contents" of a "wire communication" as those terms are defined in chapter 119 of title 18, United States Code.[33] It is the intent of this committee that pen registers do acquire "contents" of "wire communications" as those terms are defined in this bill. The term "contents" specifically mentions the identity of parties and "identity" includes a person's phone number, which can as effectively identify him as the mention of his name. Moreover, the definition of "contents" includes information concerning the "existence" of a communication. When a person dials another person's telephone number, whether or not the other person answers the phone, this is a communication under this bill. This is especially true in the intelligence field where signals to a spy may be conveyed merely by having the phone ring a designated number of times. The fact that the target of the pen registers has attempted to communicate with another person at a particular phone is information concerning the "existence" of the communication.

Of course, acquiring knowledge of the "existence" of communications in general, as opposed to acquiring knowledge of the "existence" of a particular communication or communications is not within the

[32] *United States* v. *N.Y. Telephone Co.*, —— U.S. —— (1977).

[33] This aspect of the decision seems gratuitous because the Court noted that pen registers do not result in the "aural acquisition" of anything, which would be required, to bring them under chapter 119.

term "contents." For example, acquiring knowledge that a common carrier microwave channel is in use establishes that communications "exist" on the channel but, absent any other knowledge about those communications, this would not be acquisition of "contents".

Because a major purpose of the bill is to protect privacy, nothing in the definition of "contents" is intended to preclude the retention of technical information for collection avoidance purposes. This is not inconsistent with the definition of "contents," which is intended to mean any information which may invade the privacy of a person's communications. Where information concerning the existence of communications generally, and not with respect to any particular person or group of persons or to any subject matter, is used to protect the privacy of persons' particular communications by avoiding, for example, certain radio frequencies, this furthers the privacy protections of the bill.

Section 102

Subsection (a) of this section authorizes the President, acting through the Attorney General, to approve electronic surveillances for foreign intelligence purposes without a judicial warrant in certain circumstances. As introduced, H.R. 7308 required a judicial warrant for all electronic surveillances to gather foreign intelligence. In part IV of the Committee's General Statement, *supra*, it was noted that the issue of judicial involvement in foreign intelligence surveillances was hotly debated within the committee. Some members agreed with the approach of the bill as introduced, that a warrant should be required across-the-board. Others felt that a judge should never be involved. The consensus, however, was that a judicial warrant should be required whenever the fourth amendment rights of Americans might be involved. Based on testimony taken in closed session, the committee determined that there was a class of surveillances, otherwise within the scope of the bill, where there was little or no likelihood that Americans' fourth amendment rights would be involved in any way. The committee also determined that this class of surveillances included some of the most sensitive surveillances which this Government conducts in the United States. The extreme sensitivity of those surveillances plus the fact that Americans are not involved led the committee to the decision that in this narrow class of surveillances the dangers posed to the security of these surveillances by a judicial warrant requirement were not outweighed by any competing interest of protecting the rights of Americans, because Americans were not involved. The balance was a close one, however, because other measures could minimize the dangers posed to security, while exemptions from the warrant requirement theoretically could provide a loop-hole for abuse. Accordingly, the committee has been careful to hedge this exemption from the warrant requirement with a number of strictures designed to preclude abuse, see for example, section 101(h)(4).

As was noted in part IV of the General Statement, the fact that a warrant is not required in this limited class of surveillances does not suggest congressional ratification or acknowledgement of an inherent Presidential power in the absence of legislation to conduct electronic surveillances for foreign intelligence purposes without a court order.

The authority of the President to authorize electronic surveillances without a court order in the limited class of surveillances covered by subsection (a) of this section does not derive from his powers under Article II of the Constitution, but rather from the legislation itself. The committee is of the opinion that, even if this class of surveillances involves any person's fourth amendment rights at all,[34] it is within the power of Congress to legislate a reasonable procedure for such surveillances which does not require a judicial warrant. *See*, e.g., *United States* v. *Biswell*, 406 U.S. 311 (1972); *Collonade Catering Corp.* v. *United States*, 397 U.S. 72 (1970).

Paragraph (1) of subsection (a) states that the President, through the Attorney General, may authorize electronic surveillance to gather foreign intelligence information without a court order under certain circumstances. It is intended that the President delegate to the Attorney General the day-to-day authority to approve these surveillances according to procedures adopted by the President and consistent with this bill. No particular surveillance authorized pursuant to this paragraph may continue for a period longer than 1 year without being reapproved by the Attorney General acting under the President's authorization.

To insure that only the limited class of surveillances which were brought to the attention of this committee would be authorized without a warrant, the Attorney General is required to certify in writing under oath with respect to each separate surveillance that it is solely directed at one of two different objectives. The first objective is communications exclusively between or among foreign powers as defined in section 101(a) (1), (2), or (3). The second objective is the acquisition of technical intelligence from property or premises under the open and exclusive control of a foreign power as defined in section 101(a) (1), (2), or (3). Because of the sensitive nature of these operations, the committee cannot elaborate upon the activities covered by paragraph (1)(A) of subsection (a). Through the oversight required by section 108 of the bill, the committee will insure that the activities conducted under subsection (a) without a warrant will be limited to those intended.

Paragraph (1)(B) requires the Attorney General to certify that the minimization procedures governing these surveillances meet the definition of "minimization procedures" in section 101(h). These procedures must require the destruction of any communications to which United States persons are parties and must forbid the use or disclosure of such communications, unless a court order is obtained for the surveillance or the Attorney General determines that a person's life or physical safety is endangered. See section 101(h)(4). As noted above, as a practical matter Americans' fourth amendment rights are not involved in these surveillances, but to make certain that this remains the case, this destruction requirement is made. This arrangement ensures that whenever Americans' fourth amendment rights may be involved, a court order will be required.

---

[34] By letter of April 18, 1978, the Department of Justice responded to the committee's questions by opining that foreign states and their official agents, to the extent that they are not subject to our laws, are not protected by the Fourth Amendment. Letter from John Harmon, Assistant Attorney General, Office Legal Counsel, to Chairman Boland.

As a further protection, paragraph (1) requires that the proposed minimization procedures be forwarded to the Senate and House intelligence committees at least 30 days prior to their going in effect, unless an emergency requires their immediate effect.

Paragraph (2) makes clear that surveillance authorized under this subsection without a warrant must be conducted in accordance with the Attorney General's certification and the minimization procedures approved by him. An intentional violation of this requirement would be subject to criminal penalty, see section 109.

Paragraph (3) provides for the Attorney General to direct a specified communication common carrier to render assistance so as to enable the surveillance to be successfully conducted. It parallels a like provision in chapter 119 with respect to law enforcement surveillances, see 18 U.S.C. § 2518(4), and in section 105(b)(2) of H.R. 7308 with respect to court ordered surveillances under the bill.

Subsection (b) of section 102 authorizes submission of applications to the special court (established by section 103) for an order approving the use of electronic surveillance under this title. 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 title or upon such terms and conidtions as the President wishes, so long as the terms and conditions are consistent with this title. The reference to Presidential authorization does not mean that the President has independent, or "inherent," authority to authorize electronic surveillance in any way contrary to the provisions of H.R. 7308. The procedures of this bill are the exclusive means by which electronic surveillance, as defined in section 101(f), may be conducted.

Subsection (b) also authorizes a judge to whom an application is made to grant an order for electronic surveillance, "notwithstanding any other law." Administration witnesses testified that, in their view, the activities authorized by the bill are not prohibited by the Vienna Convention on Diplomatic Relations. The committee is of the same view. It is recognized, however, that this view is one about which reasonable persons may harbor some doubt. Therefore, the "notwithstanding any other law" language is intended to make clear that, notwithstanding the Vienna Convention, the activities authorized by this bill may be conducted.

The "notwithstanding any other law" wording also deals with the contention that 28 U.S.C. section 1251, which grants the Supreme Court exclusive original jurisdiction over all actions against ambassadors of foreign states, would prevent a lower court from approving a surveillance directed at a foreign ambassador.

Subsection (b) however, makes clear that the special court does not have jurisdiction to grant orders under the circumstances described in subsection (a), unless some United States person's communication may be involved. Again, unless some United States person's communications may be involved, the Committee has determined that the balance between security and civil liberties mandates that there be no prior judicial involvement in this limited class of sensitive surveillances.

Section 103

Section 103 is a major revision of the bill's provision dealing with selection of judges who will hear applications for electronic surveillance orders. Under H.R. 7308, as introduced, seven district court judges selected by the Chief Justice would exercise nationwide jurisdiction to hear such application and three other Federal judges, similarly selected, would review denials of applications.

Subsection (a) would establish a special court with nationwide jurisdiction composed of at least one judge from each of the eleven judicial circuits nominated by the chief judges of the circuits and designated by the Chief Justice. The court would sit continuously in the District of Columbia to hear applications for electronic surveillances and exercise the duties assigned to it by section 106(f).

The creation of a special court was recommended by the General Counsel of the Administrative Office of the U.S. Courts to eliminate the jurisdictional question posed by allowing an individual Federal judge to exercise authority extending beyond his or her district. Staffing of the court with at least one judge from each circuit will provide geographical diversity, and bringing the chief judges into the selection process will promote ideological balance. Requiring the special court to sit continuously in the District of Columbia will facilitate necessary security procedures and, by ensuring that at least one judge is always available, will ensure speedy access to it by the Attorney General when timeliness is essential for intelligence purposes. The committee anticipates that only one or two judges would be in Washington, on a rotating basis, at any given time. Such a procedure would minimize judge shopping and would make it unlikely that an application for the extension of an order would be heard by the same judge who granted the original order.

Subsection (b) establishes a special court of appeals to be composed of six judges drawn from Federal courts in the vicinity of the District of Columbia who would be nominated by the chief judges of such courts and designated by the Chief Justice. The court would hear appeals from the special court and perform the duties assigned to it by section 106 (g). Any three of the judges would constitute a panel for such purposes.

The committee has provided for six judges in order to insure that a panel of three will always be available. There is no requirement that the special court of appeals sit continuously as it is anticipated that the exercise of its functions will be rare. When it must act, however, the proximity of the judges to the District of Columbia will enable the court to convene quickly.

Subsection (c) provides for 6-year terms for the judges of both courts, with the terms of the judges initially designated to be staggered. A judge may only serve two full terms.

Subsection (d) requires the chief judges of each of the special courts, in consultation with the Attorney General and the Director of Central Intelligence, to establish a wide range of security measures to protect information submitted to or produced by the courts from unauthorized disclosure. H.R. 7308, as introduced, required non-specific security measures, applicable only to the "record of proceedings". The committee's expansion of this provision reflects its concern for

the sensitivity of the intelligence information involved. Thus, consistent with the dictates of judicial independence, the committee anticipates that the document, physical, personnel, and communications security measures established by the chief judges [35] will meet the legitimate needs of the intelligence agencies.

The security provisions could include the use of executive branch personnel to perform the duties normally exercised by a court's own reporter, stenographer, or bailiff—measures suggested by the Court in the *Keith* case [36] and by the General Counsel of the Administrative Office of the United States Courts.[37]

Such provisions could also provide that responsibility for the storage of documents be undertaken by the executive branch on behalf of the court, a measure also suggested by Mr. Imlay.

Subsection (e) provides that a judge of the special court who denies an application for electronic surveillance shall record the reasons for the denial, and, upon the motion of the Government, transfer the reasons to the special court of appeals. Appeal to the special court of appeals is intended to be the exclusive means by which the Government can further pursue an application that has been denied by a judge of the special court. If, however, the Government discovers new information on which to base a new application against the same target, it may file a new application with the special court.

Subsection (f) provides that a decision of the special court of appeals shall be subject to review by the Supreme Court in the same manner as a judgment of a U.S. Court of Appeals as provided in 28 U.S.C. section 1254. The Supreme Court would be authorized to adopt special security procedures.

Subsection (g) relates to certain housekeeping details of the special courts. Specifically, it authorizes the chief judges of the special courts to designate officers or employees of the executive or judicial branches to serve as employees of the special courts. The committee believes that the work of the special courts will be of small magnitude and irregular so that there will be no need for full-time employees of the special courts. Rather designated personnel can be called upon from time to time. This subsection also authorizes the chief judges to promulgate necessary rules or administrative procedures, for example, relating to rotation of judges. The funds necessary to the special courts, which primarily should be the travel and per diem expenses of the judges, are to be drawn from Department of Justice appropriations. No change is intended with respect to what entities pay the salaries of judges and personnel designated to serve on the special courts. Finally, the Department of Justice should offer such fiscal and administrative services to the special courts as necessary, filling the role of the Administrative Office of U.S. Courts with respect to the special courts.

---

[35] The committee has designated the chief judges, rather than the Chief Justice as in H.R. 7308, as introduced, to establish the security measures to comport with the usual practice of judicial administration. The Chief Justice does not establish rules for Federal courts. See footnote 37.

[36] "Whatever security dangers clerical and secretarial personnel may pose can be minimized by proper administrative measures, possibly to the point of allowing the Government itself to provide the necessary clerical assistance." *United States* v. *United States District Court*, 407 U.S. 297, 323 (1972).

[37] Testimony of Carl H. Imlay, General Counsel, Administrative Office of the U.S. Courts, before the Subcommittee on Legislation of the House Permanent Select Committee on Intelligence, January 10, 1978.

Section 104

This section is patterned after 18 U.S.C. section 2518 (1) and (2) and specifies what information must be included in the application for a court order. Applications must be made by a Federal officer in writing and under oath or affirmation. If the officer making the application is unable to verify the accuracy of the information or representations upon which the application is based, the application should include affidavits by 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 an 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 U.S. Government and a chain of responsibility established for judicial review.

Each application must be approved by the Attorney General, who may grant such approval if he finds that the appropriate procedures have been followed. The Attorney General's written approval must indicate his belief that the facts and circumstances relied upon for the application would justify a judicial finding of probable cause that the target is a foreign power or 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 a foreign power or 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 has been made pursuant to statutory requirements.

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

Paragraph (2) requires that the application contain evidence of the authority 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, if known, or description of the person who is the target of the electronic surveillance. The words "if known" were not in H.R. 7308, as introduced, and the question was raised whether, if the Government knew the identity of the target of the surveillance, it was required to identify him. To make clear that such was required, the committee added the words "if known". The word "person" is used in its juridical sense to mean the individual or entity that is the target of the surveillance.

The word "target" is nowhere defined in the bill although it is a key term because the standards to be applied differ depending on whom or what is targeted. The committee intends that the target of a surveillance is the individual or entity about whom or from whom information is sought. In most cases this would be the person or entity at whom the surveillance is physically directed, see section 104(a)(4)(B), *infra*, but this is not necessarily so.

Generally, under the bill, targeting foreign powers may be accomplished on a less strict basis than targeting agents of foreign powers.

An individual, of course, cannot be a foreign power, only an agent of a foreign power. Therefore, if a surveillance is to be directed at an individual about whom information is sought, that individual is the target and must be shown to be an "agent of a foreign power." Where two or three individuals are associated with one another, it might be argued that they are an "association" or an "entity," which, if the proper showing is made could be considered a "foreign power." [38] This does not mean, however, that each of these individuals can then be individually surveilled merely upon a showing that together they are a "foreign power." Rather, to surveil each individually would require showing that each was an "agent of a foreign power," with its higher standard.

Often, however, associations or entities will act or communicate in a "corporate" capacity, as distinguished from the acts or communications of an individual in the association or entity. For example, corporations lease phones, enter into contracts. communicate, and otherwise act as an entity distinct from the individuals therein. The fact that an individual officer or employee, acting in his official capacity, may sign the contract or communicate with a client on behalf of the corporation does not vitiate the fact that it is the corporation rather than the individual who is acting or communicating. Thus, it is possible to target a "foreign power" in such circumstances. For instance, a corporation may lease a phone line and install a switchboard, or otherwise route the call within the organization. Assuming the corporation was a "foreign power" and the Government was seeking foreign intelligence information about the corporation itself, it could obtain an order naming the corporation as the target of a surveillance involving a wiretap of that corporation's telephone line. The committee also contemplates that it will be possible under the bill to target a "foreign power", in certain rare cases, where the facility targeted, while leased to or under the control of the entity, is in fact dedicated to the use of one particular member of the entity, for instance, where there is no switchboard but each officer has his own line with its own number. Again, however, in order to justify the target as a "foreign power" rather than as an "agent of a foreign power," the information sought must be concerning the entity, not the individual.

The judge in considering the application, wherever the Government claims the target is a "foreign power," and especially where U.S. persons are members, officers, or employees of the "foreign power," must scrutinize the description of the information sought, and the communications to be subjected to the surveillance, see section 104 (a) (6), *infra*, to determine whether the target is really the "foreign power" or rather an "agent of a foreign power." The judge must also closely scrutinize the minimization procedures to assure that where the target is a "foreign power," that individual U.S. persons who may be members or employees of the power are properly protected. In most cases it would seem possible, where a "foreign power" is the target, that individual U.S. persons who are members or employees could be protected by deleting their identities from information retained or disseminated.

[38] This would especially be true if the individuals engaged in "international terrorism" and thereby might be a group engaged in international terrorism which is a defined "foreign power."

Paragraph (4) of section 104 (a) 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 each of the facilities or places at which the surveillance is directed is being used or is about to be used by that power or agent. These requirements generally parallel existing law on surveillances for law enforcement purposes (18 U.S.C. 2518(1) (b) (ii) and (iv)).

Paragraph (5) requires a statement of the proposed minimization procedures. The statement of procedures required under this paragraph should be full and complete and normally subject to close judicial review.

It is the intention of the committee that minimization procedures be as uniform as possible for similar surveillances. The committee recognizes that certain types of surveillance operations may involve essentially identical concerns with respect to protecting U.S. persons' rights. This makes possible the adoption of uniform minimization procedures for essentially identical surveillance operations. The application of uniform procedures to identical surveillances will result in a more consistent implementation of the procedures, will result in an improved capability to assure compliance with the procedures, and ultimately means a higher level of protection for the rights of U.S. persons.

Paragraph (6) calls for a factual description of the nature of the information sought by the electronic surveillance and the type of communications or activities to be subjected to the surveillance. The description should be as specific as possible and sufficiently detailed so as to state clearly what sorts of information the Government seeks. A simple designation of which subdefinition of "foreign intelligence information" is involved will not suffice. In addition, the description should detail what type of communications and activities will be both intentionally and likely to be incidentally subjected to surveillance. Such specifics are necessary if the judge is meaningfully to assess the sufficiency and appropriateness of the minimization procedures.

Paragraph (7) requires a certification or certifications by the Assistant to the President for National Security Affairs or by another appropriate executive official appointed by the President with the advice and consent of the Senate. The certification would be made by an official having responsibility in the area of national security or foreign relations—if not the Assistant to the President, then normally the Director of Central Intelligence, the Director of the Federal Bureau of Investigation, the Secretary of Defense or such other officer, appointed with the advice and consent of the Senate, who has the appropriate knowledge to make the certification.

The possibility of additional certification is provided to insure that a detailed and complete certification is presented to the judge. The judge may, of course, require the applicant to furnish further information regarding the basis for the certification. See subsection (d) and section 105(a) (5), infra.

The certification shall state that the certifying official deems the information sought to be 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 what type of foreign intelligence information is sought and a reasoned statement of the basis for certifying that the information sought is foreign intelligence information and that such information cannot feasibly be obtained by other investigative techniques.

The requirement that the information sought be deemed "foreign intelligence information" is designed to insure that a high-level official with responsibility in the area of national security will review and explain the executive branch determination that the information sought is in fact foreign intelligence information. The requirement that this judgment be explained is to insure that those making certifications consider carefully the cases before them and avoid the temptation simply to sign off on certifications that consist largely of boilerplate language. The committee does not intend that the explanations be vague generalizations or standardized assertions. The designated official must similarly explain that the purpose of the surveillance is to obtain the described foreign intelligence information. This requirement is designed to prevent the practice of targeting, for example, a foreign power for electronic surveillance when the true purpose of the surveillance is to gather information about an individual for other than foreign intelligence purposes. It is also designed to make explicit that the sole purpose of such surveillance is to secure "foreign intelligence information", as defined, and not to obtain some other type of information. 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 U.S. citizens or resident aliens are the target of the surveillance.

Paragraph (8) requires the application to contain a statement of the means by which the surveillance will be effected. This statement should be as detailed and specific as possible in light of the need for the judge in his order to specify what activities and techniques are in fact authorized. For instance, where physical entry will be required, the application should so state indicating generally the circumstances involved.

Paragraph (9) parallels 18 U.S.C. 2518(1)(e) and requires a statement concerning all previous applications dealing with the same persons, facilities, or places, and the disposition of each such previous application.

Paragraph (10) parallels 18 U.S.C. 2518(1)(d) 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 particular information sought has been obtained, the applicant must provide facts supporting his belief that additional information of the same type will be obtained thereafter. The committee recognizes that it will be a rare case where the surveillance should terminate upon obtaining a specific set of information. Ordinarily, the information sought will not be of a type that at a given time all of it can be said to have been obtained.

Paragraph (11) was not in H.R. 7308, as introduced. The committee added it in the belief that the judge could not adequately assess the minimization procedures and assure himself that persons other

than the target identified in paragraph (3) are not in fact targets of the surveillance without a knowledge of the breadth and scope of the surveillance. For instance, one surveillance under the bill could authorize several devices or different kinds of devices placed in or directed against various different locations, all directed at the same target. Where this occurs, the judge must indeed be witting of the scope of the privacy invasion involved in order to assess properly the minimization procedures. If there are different procedures or different devices, he must also know which minimization procedures are to apply to which devices so that the order can make that clear.

As introduced, H.R. 7308's application and order requirements were divided into two separable categories, one where "foreign powers" as defined in section 101(a)(1)–(3) were the target and one where any other foreign power or any agent of a foreign power was the target. In cases involving the former category, the information provided the judge in the application and the information contained in the order were considerably abbreviated. The administration's justification for this distinction was that with respect to the "official" foreign powers in section 101(a)(1)–(3) the surveillances were much more sensitive and privacy concerns were not as great.

The committee subjected this justification to searching scrutiny. What the committee learned was that not all surveillances targeted against these "official" foreign powers were equally sensitive. Moreover, it learned that in many cases, despite the fact that the target of the surveillance was rightfully an "official" foreign power, the communications of U.S. persons generally were expected to be intercepted and that these communications were in many cases in fact sought, retained, and used. The committee is convinced that in many of these cases the acquisition, retention, dissemination, or use of such U.S. persons' communications is proper and justified. However, the committee recognized that given the limited information present in the application where "official" foreign powers were the target, the judge would not be able to have sufficient knowledge to insure that the minimization procedures adequately protected innocent U.S. persons whose communications would be intercepted.

In order to protect those surveillances which are of the utmost sensitivity, while at the same time insuring that when U.S. persons communications are involved the judge has sufficient information to make his review of minimization procedures meaningful, the committee further divided the category of surveillances targeted against "official" foreign powers into two subcategories—those in which U.S. person communications are likely to occur and where they may be retained and used, and those in which U.S. person communications are unlikely, and in any event will not be retained or used. The latter category, as explained *supra*, will not require a judicial warrant at all. In the first category, however, because U.S. persons will be involved, more information will be required to be given to the judge than was provided in H.R. 7308, as introduced, when "official" foreign powers were the target.

While section 104(a) delineates what must be in an application whenever the target of the surveillance is an "agent of a foreign power" or a "foreign power", as defined in section 101(a)(4), (5), or

(6), Section 104(b) applies only when the target of the surveillance is a "foreign power", as defined in section 101(a) (1), (2), or (3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power. In these circumstances, under section 104(b), the application need not contain: the detailed description of the information sought and the type of communications or activities to be subjected to the surveillance; the statement of the basis for the Executive certification that the information sought is the type of foreign intelligence information designated and that the information cannot be reasonably obtained by normal techniques; the statement of the means by which the surveillance will be effected; or the information required where more than one device is involved. Instead, under section 104(b), the application must contain such information about the surveillance techniques and communications or other information concerning U.S. persons likely to be obtained as may be necessary for the judge to assess the proposed minimization procedures. This insures that despite the lack of information otherwise required by subsection (a) for these surveillances, the judge will be provided with sufficient information to be able to fully assess the proposed minimization procedures. At the same time this provision protects the security of very sensitive information.

Subsection (c) of section 104 allows the Attorney General to require other executive officers to provide information to support the application.

Subsection (d) enables the judge to require the applicant to furnish further information as may be necessary to make the required determinations. It parallels existing law, 18 U.S.C. 2518(2). Such additional proffers would, of course, be made part of the record and would be subject to the security safeguards applied to the application and order.

Section 105

Subsection (a) of this section is patterned after 18 U.S.C. 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 (except where the "official" foreign powers are the target) or the minimization procedures to be followed.

Modifications in the minimization procedures should take into account the impact of inconsistent procedures on successful implementation.

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 each of the facilities or

places at which the surveillance is directed is being used or is about to be used by that power or agent.

In determining whether "probable cause" exists under this section, the court should keep in mind that this standard is not the ordinary "probable cause" that a crime is being committed, applicable to searches and seizures for law enforcement purposes. Where a U.S. person is believed to be an "agent of a foreign power," for example, there must be "probable cause" that he is engaged in certain activities, but the criminality of these activities need not always be demonstrated to the same degree. The key words—"involve or may involve"—indicate that the ordinary criminal probable cause standard does not apply with respect to the showing of criminality. For example, the activity identified by the Government may not yet involve the criminality, but if a reasonable person would believe that such activity is likely to lead to illegal activities, this would suffice. It is not intended that the Government show probable cause as to each and every element of the crime likely to be committed.

The determination by the court as to probable cause whether the person is engaging in certain activities or, for example, whether an entity is directed and controlled by a foreign government or governments, should include consideration of the same aspects of the reliability of the Government's information as is made in the ordinary criminal context—for example, the reliability of any informant, the circumstances of the informant's knowledge, the age of the information relied upon. On the other hand, all of the same strictures with respect to these matters which have developed in the criminal context may not be appropriate in the foreign intelligence context. That is, in the criminal context certain "rules" have developed or may develop for judging reliability of information. See, for example, *Spinelli* v. *United States*, 393 U.S. 410 (1969). It is not the Committee's intention that these "rules" necessarily be applied to consideration of probable cause under this bill. Rather it is the Committee's intent that in judging the reliability of the information presented by the Government, the court look to the totality of the information and consider its reliability on a case-by-case basis.

In addition, in order to find "probable cause" to believe the subject of the surveillance is an "agent of a foreign power" under subsection 101(b), the judge must, of course, find that each and every element of that status exists. For example, if a U.S. citizen or resident alien is alleged to be acting on behalf of a foreign entity, the judge must first find probable cause to believe that the entity is a "foreign power" as defined in section 101(a). There must also be probable cause to believe the person is acting for or on behalf of that foreign power and probable cause to believe that the efforts undertaken by the person on behalf of the foreign power constitute sabotage, international terrorism, or clandestine intelligence activities.

Similar findings of probable cause are required for each element necessary to establish that a U.S. citizen is conspiring with or aiding and abetting someone engaged in sabotage, international terrorism, or clandestine intelligence activities.

Finally, a proviso has been added to paragraph (3) (A) which states that no U.S. person may be considered a foreign power or an agent

of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States. This provision is intended to reinforce the intent of the committee that lawful political activities should never be the sole basis for a finding of probable cause to believe that a U.S. person is a foreign power or an agent of a foreign power. For example, the advocacy of violence falling short of indictment is protected by the first amendment, under the Supreme Court's decision in *Brandenburg* v. *Ohio*, 395 U.S. 444 (1969). Therefore, the pure advocacy of the commission of terrorist acts would not, in and of itself, be sufficient to establish probable cause that an individual or group may be preparing for the commission of such acts. However, one cannot cloak himself in first amendment immunity by advocacy where he is engaged in clandestine intelligence activities, terrorism, or sabotage.

Paragraph (4) requires the judge to find that the procedures described in the application to minimize the acquisition, retention, and dissemination of certain information or communications relating to U.S. persons fit the definition of minimization procedures. The Committee contemplates that the court would give these procedures most careful consideration. If it is not of the opinion that they will be effective, the procedures should be modified.

Paragraph (5) requires that the judges find that the application contain the statements and certifications required by section 104. If the statements and certifications conform to the requirements of section 104(a)(7), the court is not permitted to substitute its judgment for that of the executive branch officials, except where a U.S. person is the target of a surveillance. In such a case, the judge must review the certifications to determine whether they are clearly erroneous. The "clearly erroneous" standard of review is not, of course, comparable to a probable cause finding by the judge. Nevertheless, this bill does provide a workable procedure for judicial review (and possible rejection) of executive branch certifications for surveillances of U.S. persons.

H.R. 7308, as introduced, has been amended to clarify the point that the judge may base his review of the certification regarding U.S. persons not only on the statement initially submitted to him but also on any other information required by the judge to be furnished as necessary for him to determine whether or not the certification is clearly erroneous, see section 104(d) *supra*. The judge must find that the determination by the certifying official that information sought concerning a U.S. person is "foreign intelligence information" was not a clearly erroneous determination.

Despite the fact that the court is not allowed to "look behind" the certification in cases not involving U.S. persons there are several checks against the possibility of arbitrary executive action. First, the court, not the executive branch, makes the finding whether probable cause exists that the target of surveillance is a foreign power or its agent (except under section 102(a)). 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 statement and certification do not comply fully with section 104(a)(7), 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 deemed to be 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 why the information sought is foreign intelligence information which cannot reasonably be obtained through normal investigative techniques, the judge could (if the surveillance was not targeted against a foreign power as defined in section 101 (a) (1), (2), or (3)) reject the application or defer approval until an adequate certification was supplied.

Subsection (b) specifies what the order approving the electronic surveillance must contain. It must include the identity, if known, or a description of the person or persons targeted by the electronic surveillance. The order must specify each of the places or facilities against which the surveillance is directed. The order must also specify the type of information sought and the type of communications or activities to be subjected to the surveillance. These requirements are designed in light of 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, specify the means by which the surveillance will be effected. In addition, the order must specify the period of time during which the surveillance is approved. Finally, where more than one surveillance device is involved, the order must specify the authorized coverage of the devices and which minimization procedures apply to which devices.

Paragraph (2) of subsection (b) details what the court directs in the order. The order shall direct that minimization procedures will be followed. The order may also direct that a common carrier, landlord, custodian, or other specified person furnish information, facilities or technical assistance necessary to accomplish the electronic surveillance successfully and in secrecy and with a minimum of interference to the services provided by such person to the target of the surveillance. If this is done, the court shall direct that the person rendering the assistance maintain under security procedures approved by the Attorney General and the Director of the Central Intelligence Agency any records concerning surveillance which the person wishes to retain. 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 Title II of this bill. That amendment requires that before any person provides such information, facilities or technical assistance to persons authorized by law to conduct electronic surveillance, that officer is required to furnish to the person rendering the assistance either an order signed by the authorizing judge directing such assistance or, in the case of surveillance undertaken under chapter 119 or the Foreign Intelligence Surveillance Act in which a prior order is not required, such as an emergency surveillance, certification under oath by a person

specified in chapter 119 or the Attorney General that any applicable statutory requirements have been met.

The order presented to the person rendering the assistance need not be the entire order approved by the judge under this chapter. Rather only that portion of the order described in section 105(b)(2)(B)–(D), signed by the judge need be given to the specified person. This portion of the order should specify the person directed to give assistance, the nature of the assistance required, and the period of time during which such assistance is authorized.

Subsection (c) is the parallel provision to section 104(b), which makes special allowance for surveillances targeted against foreign powers as defined in section 101(a)(1), (2), or (3), where each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by such powers. When the judge has found that this is the case pursuant to section 105(a)(3), the order need not specify the type of information sought or the type of communications or activities to be subjected to the surveillance; the means by which the surveillance is to be effected; or any information with respect to whether more than one device is involved. Instead, the order must generally describe the information sought, the communications or activities to be subjected to the surveillance, and the type of electronic surveillance involved, including whether physical entry is required. Since even where "official" foreign powers are the target, American communications are intentionally sought, retained, and disseminated, the Committee wishes to emphasize that though less detail is required in an order containing a "general description," that description should delineate what information is authorized to be sought, what types of communications or activities are authorized to be subjected to surveillance, and what means of electronic surveillance are authorized to be used. The test which the judge must use to determine what a "general description" means in a particular case is what description is necessary to make clear what is authorized and not authorized. For instance, a mere designation that electronic surveillance as defined in section 101(f)(4) is authorized would be too broad, because it would authorize a wide variety of techniques, each of which might require different sorts of minimization. On the other hand, a description such as "hidden microphones to acquire oral conversations in the entire target premises" would probably suffice to generally describe the means of the surveillance and the type of communications to be subjected to the surveillance.

Subsection (d) allows an order approving electronic surveillance under this chapter against any person or entity other than an "official" foreign power as defined in section 101(a)(1), (2), or (3) 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 of these persons or entities for foreign intelligence purposes should continue without renewed 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.[40]

[40] *United States* v. *United States District Court*, 407 U.S. 297 at 323 (1972).

When the special class of "official" foreign powers is targeted, however, the surveillance may last as long as one year. Moreover, the executive determines the necessary length of the surveillance of these special foreign powers (not to exceed 1 year without reauthorization), and this determination is not subject to the court's review or approval. There are considerable arguments for this distinction between "official" foreign powers and other targets: First, the determination that an entity is within the definition of section 101(a)(1), (2), or (3) is not likely to be erroneous. Unlike a person suspected of being a foreign agent, whether an entity fits one of the three special classes of foreign powers—such as a foreign embassy or consulate—will usually be self-evident. Second, the likelihood of obtaining valuable foreign intelligence information from these entities is very high. Third, surveillance against such official powers, because of their continuing presence in the United States, is likely to be required for much longer periods of time. Although such surveillance could be accomplished by successive 90 day court renewals, the increased possibility of a security compromise as well as the administrative burden which would result, are reasons for exempting these foreign powers from the 90-day limitation. Given these considerations and the unique status of the targets involved, the committee believes that 1 year is not an excessive period of time.

As under chapter 119 of title 18, 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 104(a)(7), would therefore be required, updating the information provided previously. 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.

The committee has added a proviso to the extension provision allowing for an extension to be for a period not to exceed 1 year in the unique circumstance where the target of the surveillance is a "non-official" foreign power—those powers defined in section 101(a)(4)–(6)—and the judge finds probable cause to believe that no individual U.S. person's communications will be intercepted during the period. Where a nonofficial foreign power is the target and no individual U.S. person's communications are to be intercepted, the Committee has determined that the factors which justify a period longer than 90 days for official foreign powers are equally present. The initial order in such circumstances can only be for 90 days, during which period if no American communications are intercepted, there is likely to be probable cause that no American's communications will be intercepted in the future, thereby justifying a 1 year period for the extension.

In H.R. 7308, as introduced, there was provision for the judge in considering an application for an extension to require the Government to submit information obtained under the original order or previous extensions as might be necessary for the judge to determine whether there was probable cause that the target was a foreign power or agent thereof and that the facilities or places at which the surveillance is directed was being used or was about to be used by a foreign power or agent thereof. The committee believes that if information obtained from the prior surveillance corroborates the findings already made, the Government will wish of its own volition to tell the judge

of this to justify the extension. If there is contrary information, of course, the Government should bring this to the judge's attention, whether it was obtained by the earlier surveillance or other techniques of investigation.

It is simply unrealistic to expect the judge to review 90 days of material searching for something that may not be there. Moreover, no comparable provision exists in chapter 119 of title 18 with respect to law enforcement surveillances. Clearly, the judge has a right to information as may be necessary to his required findings, but this is already provided for in section 104(d). For these reasons, the committee has deleted the provision as it appeared in H.R. 7308, as introduced.

On the other hand, in order to make clear the scope of the judge's authority to review compliance with the minimization procedures, a provision has been added at the end of subsection (d). It provides that at the end of the period of time for which an electronic surveillance is approved by an order or an extension issued under this section, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning U.S. persons was acquired, retained, or disseminated. This provision is not intended to require that the judge assess such compliance, nor is it intended to limit such assessments to any particular intervals. The committee believes, however, that it is useful to spell out the judge's authority explicitly so that there will be no doubt when a judge may review the manner in which information about U.S. persons is being handled. This specifically includes information about U.S. persons acquired from electronic surveillance of a foreign power, as defined in section 101(a) (1), (2), or (3), except when it is a surveillance approved pursuant to section 102a); then the judge has no authority to review the minimization under the procedures approved by the Attorney General and reported to the Senate and House Intelligence Committees.

Subsection (e) 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 employment 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 title 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. 2518(7). First, only the Attorney General—as defined—may authorize such emergency surveillance, whereas in 18 U.S.C. 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. 2518 (7). Third, an application for an order approving the surveillance must be made to that judge within 24 hours; 18 U.S.C. 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. 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 title 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). This last provision is designed to insure that as much as possible be done to eliminate the acquisition, retention, and dissemination of information which does not relate to foreign intelligence purposes. The committee's intent is to place the Attorney General in the role of the court during the 24-hour emergency period. He must examine the minimization procedures as the court would normally do under paragraph (a) (4) of this section, and ensure that the appropriate procedures are followed.

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 insures that all emergency surveillance initiated pursuant to this title 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 24-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 Department of Justice and congressional intelligence 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 103, 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 title 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 obtained, 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.

In addition, no information concerning any U.S. person acquired from a disapproved emergency surveillance may subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General where the information indicates a threat of death or serious bodily harm. The fact that an emergency surveillance was conducted improperly should not disable the Government from using the information to protect the life or physical safety of a person.

A denial of the application may be reviewed in the same manner as a denial of an original application under section 103.

Subsection (f) creates statutory authorization for three types of activities which, under certain circumstances, may technically involve "electronic surveillance," as defined in section 101(f). These three activities are the testing of electronic equipment, the conducting of "sweeps" to discover illegal taps or bugs, and the training of personnel on electronic surveillance equipment.

No warrant is required for these activities given the fact that they are not targeted against any particular person or persons and the fact that the bill's restrictions on these activities are so strict that there is no reasonable possibility of abuse.

Under H.R. 7308, as introduced, a similar provision was, by a conforming amendment, placed in chapter 119 of title 18 rather than in this title. The committee believes, however, that inasmuch as the need for this provision was the result of the limitations of this title and that intelligence agencies will be the primary, if not the sole, users of this authorization, this provision should be in this title rather than chapter 119 which deals with law enforcement surveillances.

Several changes have been made to the comparable provision in H.R. 7308, as introduced. First, no provision was made in H.R. 7308, as introduced, for training. Second, consistent with E.O. 12036, January 24, 1978, tests, "sweeps," and training must be conducted pursuant to procedures approved by the Attorney General.[41] Second, no test, "sweep", or training may be targeted against the communications of a particular person or persons.[42] Third, tests, "sweeps", and training under this provision are only authorized if it is not reasonable to obtain the consent of the persons who might be incidentally intercepted. In certain situations it may be possible to obtain the consent of at least one party, such that the activity would no longer be "electronic surveillance" as defined in section 101(f). Obtaining such consent is preferred.

For example, where certain telephone lines are to be "swept" to check for "taps," it may be possible to obtain the consent of the persons whose lines these are. Finally, there are strict limitations on the use of information which might be acquired by surveillance authorized by this subsection. Specifically, the information must be used only to determine the capability of the equipment tested, or to enforce the law against unlawful surveillance or protect information from unauthorized surveillance, as appropriate. Where training is involved, there are further restrictions that the authority of this subsection may not be used either where it is reasonable to train the persons in the course of surveillance otherwise authorized by the bill, for example, during testing or during a court ordered surveillance, or where it would be reasonable to train the persons in a manner which would not involve "electronic surveillance," as defined, for example, outside the United States or in laboratory conditions. The committee recognizes that it would be unreasonable to require persons to be trained in using equipment under circumstances where a slip-up might result in their arrest by foreign police or the disclosure of their sophisticated equipment.

[41] This eliminates the need for Attorney General approval of tests that continue longer than 90 days.

[42] This does not mean that a test, "sweep", or training cannot be aimed at communications carried by a particular common carrier. Here, "communications of" a particular person means communications to which a particular person is a party.

The committee also recognizes that training in laboratory conditions may not be sufficient; field training in almost all areas of endeavor is considered necessary. Finally, communications acquired in the course of training personnel are barred from being retained or disseminated. There is no need for anyone other than the trainees and their instructor to have any knowledge of what might or might not have been intercepted.

The authorization in this subsection is a narrow one made necessary by the broad definition of "electronic surveillance." It is not intended to authorize electronic surveillances to gather foreign intelligence information generally. Thus the provision is phrased in terms of the purpose being "solely to test the capability of electronic equipment . . . , determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance . . . or training intelligence personnel in the use of electronic surveillance equipment." Where, for example, the existence and capability of unauthorized electronic surveillance equipment has been established, this provision does not authorize further surveillance to determine the targets of the surveillance or the information being acquired by the unauthorized surveillance.

All tests, "sweeps" and training conducted pursuant to this provision must be in the normal course of official business by the Government agent conducting the test, sweep, or training. The committee contemplates that such testing, "sweeps," and training will be approved by a senior official prior to the commencement of the activity.

Subsection (g) was not in H.R. 7308, as introduced. Its effect is self-explanatory. It's purpose is to assure accountability by requiring that applications and orders be maintained for 10 years. Under chapter 119 of title 18, U.S.C., there is a similar 10 year recordkeeping requirement.

Section 106

This section places additional constraints on Government use of information obtained from electronic surveillance and establishes detailed procedures under which such information may be received in evidence, suppressed, or discovered.

Subsection (a) requires that information concerning U.S. persons acquired from electronic surveillance pursuant to this title may be used and disclosed by Federal officers and employees, without the consent of the U.S. person, only in accordance with the minimization procedures defined in section 101(h). This provision ensures that the use of such information is carefully restricted to actual foreign intelligence or law enforcement purposes.

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 (a) further states that no information (whether or not it concerns a U.S. person) acquired from an electronic surveillance

pursuant to this title may be used or disclosed except for lawful purposes. This provision did not appear in H.R. 7308, as introduced. It was added by the committee to insure that information concerning foreign visitors and other non-U.S. persons, the use of which is not restricted to foreign intelligence or law enforcement purposes, is not used for illegal purposes.

There is no specific restriction in the bill regarding to whom Federal officers may disclose information concerning U.S. persons acquired pursuant to this title although specific minimization procedures might require specific restrictions in particular cases. 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 title 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 Government channels. For example, Federal agents may learn of a terrorist plot to kidnap a business executive. Certainly in such cases they should be permitted to disclose such information to the executive and his company in order to provide for the executive's security.

Finally, the committee believes that foreign intelligence information relating to crimes, espionage activities, or the acts and intentions of foreign powers may, in some circumstances, be appropriately disseminated to cooperating intelligence services of other nations. So long as all the procedures of this title are followed by the Federal officers, including minimization and the limitations on dissemination, this cooperative relationship should not be terminated by a blanket prohibition on dissemination to foreign intelligence services. The committee wishes to stress, however, that any such dissemination be reviewed carefully to ensure that there is a sufficient reason why disclosure of information to foreign intelligence services is in the interests of the United States.

Disclosure, in compelling circumstances, to local officials for the purpose of enforcing the criminal law, to the targets of clandestine intelligence activity or planned violence, 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.

It is recognized that these strict requirements only apply to information known to concern U.S. persons. Where the information in the communication is encoded or otherwise not known to concern U.S. persons, only the requirement that the information be disclosed for lawful purposes applies. There is no requirement that before disclosure can be made information be decoded or otherwise processed to determine whether information concerning U.S. persons is indeed present. Of course, the restrictions on use and disclosure still apply, so that if any Government agency received coded information from the intercepting agency, were it to break the code, the limitations on use and disclosure would apply to it.

Subsection (b) requires that disclosure of information for law enforcement purposes must be accompanied by a statement that such

evidence, or any information derived therefrom, may be used in a criminal proceeding only with the advance authorization of the Attorney General. This provision is designed to eliminate circumstances in which a local prosecutor has no knowledge that evidence was obtained through foreign intelligence electronic surveillance. In granting approval of the use of evidence the Attorney General would alert the prosecutor to the surveillance and he, in turn, could alert the court in accordance with subsection (c) or (d).

Subsections (c) through (i) set forth the procedures under which information acquired by means of electronic surveillance may be received in evidence or otherwise used or disclosed in any trial, hearing or other Federal or State proceeding. Although the primary purpose of electronic surveillance conducted pursuant to this chapter is not likely to be the gathering of criminal evidence, it is contemplated that such evidence will be acquired and these subsections establish the procedural mechanisms by which such information may be used in formal proceedings.

At the outset the committee recognizes that nothing in these subsections abrogates the rights afforded a criminal defendant under *Brady* v. *Maryland*,[43] and the Jencks Act.[44] 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 at trial.[45]

Subsection (c) states that no information acquired from an electronic surveillance (or any fruits thereof) may be used against an aggrieved person, as defined, 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 United States notifies the court or other authority and the aggrieved person of its intent.

Subsection (d) places the same requirements upon the states and their political subdivisions, and also requires notice to the Attorney General.

Subsection (e) provides a separate statutory vehicle by which an aggrieved person against whom evidence derived or obtained from an electronic surveillance is to be or has been introduced or otherwise used or disclosed in any trial, hearing or proceeding may move to suppress the information acquired by electronic surveillance or evidence derived therefrom. The grounds for such a motion would be that (1) the information was unlawfully acquired, or (2) the surveillance was not made in conformity with the order of authorization or approval.

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

It should be noted that the term "aggrieved person", as defined in section 101(k) does not include those who are mentioned in an intercepted communication. The committee wishes to make it clear that

[43] 373 U.S. 83 (1963).
[44] 18 U.S.C. 3500 et seq.
[45] *United States* v. *Andolschek*, 142 F.2d 503 (2nd Cir. 1944).

such persons do not have standing to file a motion under section 106 or under any other provision. The minimization procedures do apply to such persons and, to the extent that such persons lack standing, the committee recognizes that it has created a right without a remedy. However, it is felt that the Attorney General's regulations concerning the minimization procedures, judicial review of such procedures, and criminal penalties for intentional violation of them, will provide sufficient protection.

Section (f) sets out special judicial procedures to be followed when the Government concedes that it intends to use or has used evidence obtained or derived from electronic surveillance. Where, in any trial or proceeding, the Government concedes, either pursuant to the notification [46] requirements of subsection (c) and (d) or after a motion is filed by the defendant pursuant to subsection (e), that it intends to use or has used evidence obtained or derived from electronic surveillance, it may make a motion before the special court to determine the lawfulness of the surveillance. The special court must then determine whether the surveillance was lawful or not. In so doing, no judge who granted an order or extension involving the surveillance at issue could make the determination, unless all the judges of the special court would be so disqualified.

The determination would be made in camera if the Attorney General certifies under oath that disclosure would harm the national security or compromise foreign intelligence sources and methods.[47] However, when the special court determines that there is a reasonable question as to the legality of the surveillance and disclosure would likely promote a more accurate determination thereof (or when the court determines that disclosure would not harm the national security) the defendant should be provided relevant portions of the application, order, or other materials. Whenever there is a reasonable question of legality, it is hoped that disclosure, with an in camera adversary hearing, will be the usual practice. The committee considered requiring an adversary hearing in all cases, but was persuaded by the Department of Justice that in those instances where there is no reasonable question as to the legality of the surveillance security considerations should prevail. In ordering disclosure, the special court must provide for appropriate security procedures and protective orders.

Subsection (f), outlined above, deals with those rare situations in which the Government states it will use evidence obtained or derived from an electronic surveillance.

Subsection (g) states in detail the procedures to be followed when, in any court or other authority of the United States or a state, a motion or request is made to discover or obtain applications or orders, or other materials relating to surveillance under this title, or to dis-

[46] It should be emphasized that notification by the Government triggers the special court procedures whether or not the defense has filed a suppression or discovery motion. Thus, if, before the filing of such motions, the Government concedes use of evidence obtained from electronic surveillance, and the Court determines that the surveillance was lawful, a discovery or suppression motion would be moot because of the requirements of subsection (h).

[47] In many, if not most cases, the Attorney General's affidavit will have to be based on information supplied to him by other Executive officers. It is perfectly proper for the Attorney General in making his affidavit to rely on conclusions and beliefs held by others in the Executive Branch who are responsible for national security or intelligence sources and methods.

cover, obtain or suppress any information obtained from electronic surveillance, and the Government certifies that no information obtained or derived from an electronic surveillance has been or is about to be used by the Government before that court or other authority.

When such a motion or request is made, it will be heard by the Special Court of Appeals if:

The court or other authority in which the motion is filed determines that the moving party is an aggrieved person, as defined;

The Attorney General certifies to the Special Court of Appeals that an adversary hearing would harm the national security or compromise intelligence sources or methods; and;

The Attorney General certifies to the Special Court of Appeals that no information obtained or derived from an electronic surveillance has been or is to be used.

If the above findings and certifications are made, the special court of appeals will stay the proceedings before the court or other authority and conduct an ex parte, in camera inspection of the application, order or other relevant material to determine whether the surveillance was lawfully authorized and conducted.

The subsection further provides that in making such a determination, the court may order disclosed to the person against whom the evidence is to be introduced the court order or accompanying application, or portions thereof, or other materials relating to the surveillance, only if it finds that such disclosure is necessary to afford due process to the aggrieved person.

It is to be emphasized that, although a number of different procedures might be used to attack the legality of the surveillance, it is the procedures set out in subsections (f) and (g) "notwithstanding any other law" that must be used to resolve the question. The committee wishes to make very clear that these procedures apply whatever the underlying rule or statute referred to in the motion. This is necessary to prevent these carefully drawn procedures from being bypassed by the inventive litigant using a new statute, rule or judicial construction.

Subsections (f) and (g) effect substantial changes from H.R. 7308, as introduced. The committee has adopted a suggestion of the General Counsel of the Administrative Office of the U.S. Courts in providing that judicial determinations with respect to challenges to the legality of foreign intelligence surveillances and motions for discovery concerning such surveillances, where the Government believes that adversary hearings or disclosure would harm the national security, will be made by the special court or the special court of appeals. Given the sensitive nature of the information involved and the fact any judge might otherwise be involved in situations where there would be no mandated security procedures, the committee feels it appropriate for such matters to be considered solely by the special courts.

Moreover, judges of the special courts are likely to be able to put claims of national security in a better perspective and to have greater confidence in interpreting this bill than judges who do not have occasion to deal with the surveillances under this bill, and the Government is likely to be less fearful of disclosing information even to the judge where is knows there are special security procedures and the judge already is cognizant of other foreign intelligence surveillances. These

considerations, it is believed, suggest that—given the in camera procedure—the private party will be more thoroughly protected by having the special courts determine the legality of the surveillances under the bill.

The most significant change is contained in the subsection (f) provision authorizing disclosure and an adversary hearing in certain circumstances. This provision has been adopted only after lengthy discussion within the committee and a careful consideration of the suggested risk to security involved. The narrow reach of the provision should be emphasized: the adversary hearing procedures can arise only in those instances where the Government concedes that it intends to use evidence obtained or derived from an electronic surveillance (which the Government had not done in the last 10 years until the case of *U.S.* v. *Humphrey*, crim. no. 78–25–A, E.D. Va.).

Furthermore, the decision to remove a proceeding to one of the special courts (under subsection (f) or (g)), is entirely up to the Government in the first instance, as, of course, is the decision to prosecute. With these limitations, the committee believes that the adversary hearing provision is fully protective of those legitimate security interests which the Congress, no less than the executive branch, has a duty to safeguard.

The Congress has an equally compelling duty to insure that trials are conducted according to traditional American concepts of fair play and substantial justice. In this context, the committee believes that when the Government intends to use information against a criminal defendant obtained or derived from an electronic surveillance, and there is a reasonable question as to the legality of a surveillance, simple justice dictates that the defendant not be denied the use of our traditional means for reaching the truth—the adversary process.[49]

Where the Government states under oath that it does not intend to use evidence or information obtained or derived from electronic surveillance, the case for an adversary hearing is less persuasive and the bill does not provide for it. In such cases, however, in order to provide additional protection to the defendant, the bill (if the case is removed from the trial court) states that the matter be heard by three judges of the special court of appeals, rather than by a single judge of the special court.

It should be emphasized that in determining the legality of a surveillance under subsection (f) or (g), the judges of the special courts (or the trial judge if the matter is not removed to the special courts) are not to make determinations which the issuing judge is not authorized to make. Where the bill specifies the scope or nature of judicial review in the consideration of an application, any review under these subsections is similarly constrained. For example, when reviewing the certifications required by section 104(a)(7), unless there is a prima facie

[49] The committee is aware that the Supreme Court has never decided that an adversary hearing is constitutionally required to determine the legality of a surveillance. See *Alderman* v. *United States*, 394 U.S. 165 (1968); *United States* v. *Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc), cert. denied sub nom. *Ivanov* v. *United States*, 419 U.S. 881 (1974); *Giordano* v. *United States*, 394 U.S. 310, 314 (1968) (concurring opinion of Justice Stewart.) This fact does not lessen the importance of an adversary hearing in searching for the truth and assuring a fair trial, and if the court should so decide, the procedures for an adversary hearing would already be in place. It should also be noted that in neither *Alderman* nor *Butenko* did the Government concede use of information obtained or derived from a surveillance.

showing of a fraudulent statement by a certifying officer, procedural regularity is the only determination to be made if a non-U.S. person is the target, and the "clearly erroneous" standard is to be used where a U.S. person is targeted. Of course, the judge is also free to review the constitutionality of the law itself.

Subsection (h) states what procedures the special courts are to follow after a determination of legality or illegality is made pursuant to subsection (f) or (g). The committee wishes to emphasize that its intent in this provision is not to legislate new procedures or in any other manner alter existing procedures with respect to what should be ordered after a finding of illegality is made. In such circumstances, the judge is directed to suppress the evidence or otherwise grant the motion "in accordance with the requirements of law." Existing case law requires the Government, in the case of an illegal surveillance, to surrender to the defendant all the information illegally acquired in order for the defendant to make an intelligent motion on the question of taint. The Supreme Court in *Alderman* v. *United States*, *supra*, held that once a defendant claiming evidence against him was the fruit of unconstitutional electronic surveillance has established the illegality of such surveillance (and his "standing" to object), he must be given those materials illegally acquired in the Government's files to assist him in establishing the existence of "taint." The Court rejected the Government's contention that the trial court could be permitted to screen the files in camera and give the defendant only material which was "arguably relevant" to his claim, saying such screening would be sufficiently subject to error to interfere with the effectiveness of adversary litigation of the question of "taint." The Supreme Court has refused to reconsider the *Alderman* rule and, in fact reasserted its validity in its *Keith* decision. (*United States* v. *U.S. District Court*, *supra*, at 393).

As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

A decision of illegality may not always arise in the context of suppression; rather it may, for example, arise incident to a discovery motion in a civil trial. Here, again, the bill does not specify what the court should order. Again, the court should grant the motion only "in accordance with requirements of law." Here, however, the requirements of law would be those respecting civil discovery. In other words, once the surveillance is determined to be unlawful, the intent of this section is to leave to otherwise existing law the resolution of what, if anything, is to be disclosed. For instance, under the Freedom of Information Act, other defenses against disclosure may be able to be made.

Where the court determines pursuant to subsections (f) or (g) that the surveillance was lawfully authorized and conducted, it would, of course, deny any motion to suppress. In addition, once a judicial determination is made that the surveillance was lawful, any motion or request to discover or obtain materials relating to a surveillance must

be denied unless disclosure or discovery is required by due process.[50]

Subsection (i) states for purposes of appeal that orders or decisions of the special courts granting or denying motions, deciding the lawfulness of a surveillance or ordering or denying disclosure shall be final orders, and shall be binding upon all courts of the United States and the States except the special court of appeals and the Supreme Court. As final orders they will be immediately appealable, by the private party or the government. The committee recognizes that the usual practice is to consider such orders interlocutory and not immediately appealable.

In the particular circumstances of cases handled pursuant to subsections (c)–(i), however, the committee believes that substantial considerations militate in favor of immediate appeal. Requirements to disclose certain information, whether before or after a finding of illegality, might force the Government to dismiss the case (or concede the case, if it were a civil suit against it) to avoid disclosure it thought not required. This is not the situation in normal cases, and therefore it is appropriate here to allow immediate appeal of such an order. Similarly, given the in camera and to a greater or lesser extent ex parte proceedings under subsections (f) and (g), it is appropriate to afford a more expeditious form of appeal for the private litigant. Because cases under these subsections are not expected to occur often, there is no meaningful added burden placed on the courts by allowing such interlocutory orders.

New subsection (j) has been added to the bill for the purpose of restricting the use of unintentionally acquired private domestic radio communications. The new subsection is needed because "electronic surveillance" as defined in 101(f)(3) covers only the intentional acquisition of the contents of private domestic radio communications. Such communications may include telephone calls and other wire communications transmitted by radio microwaves. Concern has been expressed that unless the use of such unintentionally acquired communications is restricted, there would be a potential for abuse if the Government acquired those kinds of domestic communications, even without intentionally targeting any particular communication. The amendment forecloses this possibility by restricting the use of any information acquired in this manner.

In circumstances involving the unintentional acquisition, by an electronic, mechanical, or other surveillance device of the contents of any radio communication, where a persons has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and where both the sender and all intended recipients are located within the United States, the contents must be destroyed upon recognition. The only exception is with the approval of the Attorney General where the contents indicate a threat of death or serious bodily harm to any person. This restriction is not intended to prevent the Government from maintaining a record of the radio frequency of the communication for later collection avoidance purposes.

[50] The committee recognizes that this provision alters existing law and is a limitation on existing discovery practice. It is felt that where the special court has determined that the surveillance is lawful, security considerations should preclude any disclosure unless due process requires disclosure.

Subsection (k) provides for notice to be served on U.S. 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 are 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 information was or was not obtained. This notice may be postponed for a period of up to 90 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 court order 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 has 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 ongoing foreign intelligence investigation because of the logical inferences a foreign intelligence service might draw from the targeting of the individual. For these reasons, the Government is given the opportunity to present its case to the judge for initially postponing notice. After 90 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 107

Section 107 requires the submission of annual reports to both the Congress and the Administrative Office of the U.S. Courts containing statistical information relating to electronic surveillance under this title. The reports must include the total number of applications made for orders and extensions and the total number of orders or extensions granted, modified, and denied, The statistics in these reports should present a quantitative indication of the extent to which surveillance under this title is used. The committee intends that such statistics will be public.

Section 108

Congressional oversight is particularly important in monitoring the operation of this statute. By its very nature foreign intelligence surveillance must be conducted in secret. The 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, contrary to the premises which underlie the provisions of title III of the Omnibus Crime Con-

trol Act of 1968, it is contemplated that few electronic surveillances conducted pursuant to this title will result in criminal prosecution.

For these reasons, the committee has added a new section to the bill dealing with the information to be furnished to the appropriate congressional committees. Section 108 requires the Attorney General to inform fully the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence concerning all electronic surveillance under this title. He must do so at least semiannually.

As interpreted by the committee, the word "fully" means that the committee must be given enough information to understand the activities of, but does not mean that the Attorney General must set forth each and every detailed item of information relating to, all electronic surveillances. For example, the committee would not ordinarily wish to know the identities of particular individuals. The committee and the Department of Justice have had lengthy discussions concerning this provision and are in general agreement as to what information will be provided. To preserve the Intelligence Committees' right to seek further information, when necessary, section 108 makes clear that nothing in this title shall be deemed to limit the authority of those committees to obtain such additional information as they may need to carry out their respective functions and duties. In the case of the House Permanent Select Committee on Intelligence, that authority is set forth in House Resolution 658, 95th Congress, 1st session.

Section 109

Section 109(a)(1) carries forward the criminal provisions of chapter 119 and makes it a criminal offense for officers or employees of the United States to intentionally engage in electronic surveillance under color of law except as specifically authorized in chapter 119 of title III and this title. Since certain technical activities—such as the use of a pen register—fall within the definition of electronic surveillance under this title, but not within the definition of wire or oral communications under chapter 119, the bill provides an affirmative defense to a law enforcement or investigative officer who engages in such an activity for law enforcement purposes in the course of his official duties, pursuant to a search warrant or court order.[51] Section 109(a)(2), is a new provision (not found in chapter 119 or H.R. 7308 as introduced) which makes it a criminal offense for any officer or employee of the United States to intentionally violate any order issued pursuant to this title or to intentionally violate the sections specified, knowing that his conduct violates such order or title. The sections covered are generally those pertaining to the use and disclosure of information obtained from electronic.

Section 109(a)(2) generated considerable debate within the committee and was adopted only after full consideration was given to its suggested deleterious effect on the morale of intelligence personnel.

One of the important purposes of the bill is to afford security to intelligence personnel so that if they act in accordance with the statute and the court order, they will be insulated from liability; it is not to afford them immunity when they intentionally violate the law.

[51] See *U.S.* v. *New York Telephone Company*, —— U.S. —— (1977), 46 LW 4033.

Absent this criminal provision, intelligence agency personnel—agents and supervisors alike—could intentionally and totally ignore the minimization procedures and be immune from criminal or civil liability. Moreover, they could intentionally destroy records required by the bill to be retained for oversight purposes without fear of liability. While chapter 119, dealing with law enforcement surveillances, does contain a penalty for violations of use and disclosure restrictions on information lawfully obtained, the committee feels that the strict probable cause standard for a chapter 119 surveillance lessens the importance of minimization and restrictions on disclossure as a safeguard against abuse. On the other hand, the lesser showing required for a foreign intelligence surveillance warrant makes the minimization and other procedures dealing with disclosure of information extremely important, and thus sanctions should apply to intentional violations of such provisions.

The word "intentionally" was carefully chosen. It is intended to reflect the most strict standard for criminal culpability. What is proscribed is an intentional violation of an order or one of the specified provisions, not just intentional conduct. The Government would have to provide beyond a reasonable doubt both that the conduct engaged in was in fact a violation, and that it was engaged in with "a conscious objective or desire" [52] to commit a violation. The phrase "knowing his conduct violates such an order or this title" is intended to emphasize this point. To further insure that intelligence personnel are protected in the proper performance of legitimate duties, the bill provides a "good faith" defense.

Theoretically, because the definition of electronic surveillance in this title includes most activities encompassed within the term "interception of wire or oral communication" in chapter 119, a single offense could violate both 109(a)(1) and the criminal provision of chapter 119. The committee intends that in such cases the Government proceed under only one of the provisions, not both.

In addition to making an intentional violation of the disclosure and minimization provisions a criminal offense the reported bill differs from H.R. 7308 (as introduced) by including the criminal (and civil) liability provisions in the body of this title rather than amending chapter 119. The purpose of this change is to minimize the multiplicity of cross references to chapter 119 and to alleviate the confusion caused by having chapter 119's criminal provisions apply to this title and to minimize the effects of this title on chapter 119 law enforcement surveillances. For example, under H.R. 7308, as introduced, it would have been a federal crime for a State law enforcement officer to use a pen register without a warrant. While such action may be unconstitutional, it is not made a criminal offense by chapter 119 and should not be by this title.

(For the same reasons, section 110 makes the civil liability provisions a part of this title.)

The methodology of the criminal provision of section 109 reflects the committee's efforts to conform to the methodology of the pending criminal code reform legislation (H.R. 6869/S. 1437).

[52] The phrase "conscious objective or desire" is taken from the definition of "intentional" contained in section 302 of S. 1437 (the Criminal Code Reform Act of 1978) as passed by the Senate on January 30, 1978.

Section 110

This section imposes civil liability for violations of section 109(a)(1) and section 109(a)(2), and authorizes an "aggrieved person", as defined in section 101(k), to recover actual damages, punitive damages, and reasonable attorney's fees and costs. Since the civil cause of action only arises in connection with a violation of the criminal provision, the statutory good faith defense, though applicable, does not have to be restated. Although included in the definition of "aggrieved person", foreign powers and non-U.S. persons who act in the United States as officers or employees of foreign powers would be prohibited from bringing actions under section 110.

The agent of a foreign power exclusion of section 110 is narrower than the corresponding provision of H.R. 7308, as introduced. The exclusion only applies to those who come within the definition of agent of a foreign power because they act in the United States as an officer, member or employee of a foreign power, see section 110(b)(1)(A). The foreign visitors covered by the second part of the defintion, see section 110(b)(1)(B) would have a cause of action under the provision. The original bill excluded both of these classes of agents of a foreign power. The committee believes that the lesser exclusion is more appropriate. As regards the first category those barred from the civil remedy will be primarily those persons who are themselves immune from criminal or civil liability because of their diplomatic status. In regard to the second category it is difficult to see what would be gained by denying the civil remedy in practical terms. In proving that the exclusion applied the Government would more than likely be forced to make the same showing that it would make in proving that the surveillance was lawful.

TITLE II

Title II contains the conforming amendments necessary to integrate the Foreign Intelligence Surveillance Act into the existing provisions of chapter 119 of title 18. In adopting its other amendments, one of the committee's purposes has been to produce legislation that can be read and understood (and thus complied with) easily, without excessive cross reference to other statutes. Thus, for example, the committee has expanded the definition section and provided the bill with its own criminal and civil liability and testing and countermeasures provisions. As a result, most of the conforming amendments contained in H.R. 7308, as introduced, have been eliminated.

Section 201(a)

This provision rewrites existing section 2511(2)(a)(ii) of title 18, United States Code, which states that "it shall not be unlawful under this chapter" for a communications common carrier to assist law enforcement and investigative officers in performing surveillance activities pursuant to title 18. Section 201(a) would restate this provision in terms of an authorization, rather than an exemption from criminality, and would include "landlords, custodians, or other persons" in the authorization, extend its scope to cover foreign intelligence electronic surveillance, require the Government to provide a copy of the

Attorney General certification or portions of the court order and other information to the person rendering assistance, relieve such person from all civil liability for actions in conformance with the court order or certification, and prohibit such person from divulging the existence of a surveillance or the device involved (unless required by legal process and after notice has been given to the Attorney General or oppropriate state official).[53]

Section 2511(2)(a)(ii) was added to chapter 119 in 1970 in response to the telephone company's refusal to provide assistance to officers engaged in court ordered wiretaps on the theory that such assistance would constitute a violation of the Communications Act of 1934 and chapter 119, At the same time, section 2518(4)(e) was added, authorizing the judge issuing the warrant to order a "communication common carrier, landlord, custodian, or other person" to provide assistance. The committee has made the two provisions consistent in terms of those who are authorized to provide assistance and those whom a judge can order to provide assistance.

The provision prohibiting the disclosure of the existence of a surveillance or the surveillance technique was added by the committee. It is necessary in light of the practice of some telephone companies to inform customers who request a line check that there is a wiretap on their phone, whether or not the tap was lawfully authorized.

Where a court order is required to initiate a surveillance, a copy of the order must be provided to the party providing assistance. Where a court order is not required, a copy of the relevant Attorney General certificate must be provided. Examples of the latter would be emergency surveillances under section 105(e), surveillances conducted under the special circumstances of section 102(a), and surveillances conducted pursuant to the testing, counter-measures and training provisions of section 105(f).

Requiring the court order or certification to be presented before the assistance is rendered serves two purposes. It places an additional obstacle in the path of unauthorized surveillance activity, and, coupled with the provision relieving the third party from liability if the order or certification is complied with, it provides full protection to such third parties. In the past, phone companies have been subjected to civil suits for rendering assistance to the Government, whether or not a court order was involved. The committee provision is intended to hold harmless the phone company and others so long as the assistance is in accordance with the terms of the order or certification, even if the surveillance is later found to be unlawful.

The court order or certification must indicate the period of time during which the provision of information, facilities or technical assistance is authorized and must specify the information, facilities or technical assistance required. These requirements are more detailed than the corresponding provision of H.R. 7308, as introduced. They will eliminate any doubts the party providing assistance might harbor concerning what is required of him and what are the limits of his authority.

---

[53] The notice provision is intended to provide sufficient time for the Government to intervene to quash a subpoena or otherwise take legal action to prevent disclosure if it so desires.

A further change from H.R. 7308, as introduced, is contained in the provision empowering the specified third parties to provide assistance to "persons authorized by law to intercept wire or oral communications or to conduct electronic surveillance . . .". H.R. 7308, as introduced, would not have changed the existing language of chapter 119, which authorizes third party assistance to "law enforcement or investigative officers." The latter phrase is a defined term in chapter 119 and is not appropriate to designate those who will conduct electronic surveillance under the Foreign Intelligence Surveillance Act of 1978.

The language selected by the committee is intended to include only those individuals empowered by chapter 119 to intercept wire or oral communications for law enforcement purposes and those empowered by the Foreign Intelligence Surveillance Act of 1978 to engage in electronic surveillance for foreign intelligence purposes, and should not be subject to any broader interpretation.

Section 201(b)

This provision adds two subsections to section 2511(2) of title 18.

New subsection (e) makes explicit that the criminal penalties of chapter 119 of title 18 and the prohibitions of the Communications Act of 1934 do not apply to those engaging in electronic surveillance pursuant to title I of the Foreign Intelligence Surveillance Act.

New subsection (f) must be read in conjunction with the conforming amendment contained in section 201(c) which repeals section 2511(3) of title 18. The effect of these two conforming amendments is to establish the Foreign Intelligence Surveillance Act as the exclusive legislative statement on the question of the Executive's power to order electronic surveillance.

Subsection (f) begins by stating that nothing contained in chapter 119 or section 605 of the Communications Act of 1934, shall be deemed to affect the acquisition of foreign intelligence information from international or foreign communications by a means other than electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978.

This provision is designed to make clear that the legislation does not deal with certain international signals intelligence activities currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States.

The second part of new subsection (f) is a directive to Government officials. It states that with respect to the interception of domestic wire and oral communications, and to electronic surveillance, as defined in section 101(f), the procedures of chapter 119 and of the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which such activities may be conducted.[54]

[54] As noted earlier, the use of pen registers and similar devices for law enforcement purposes is not covered by chapter 119 or this Act and new subsection (f) is not intended to prohibit it. Rather, because of the criminal defense provision of section 109(b)(1), the "procedures" referred to in subsection (f) include acquiring a court order for such activity. It is the Committee's intent that neither this nor any other provision of the legislation have any effect on the holding in *United States* v. *New York Telephone*, —— U.S. —— (1977), 46 LW 4033 that rule 41 of the Federal Rules of Criminal Procedure empowers federal judges to authorize the installation of pen registers for law enforcement purposes.

Article I, section 8, of the Constitution states:

> The Congress shall have Power * * * To make all laws which shall be necessary and proper for carrying into Execution the foregoing power, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof.

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 explicity 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).

Thus, despite any inherent power of the President to authorize warrantless electronic surveillances in the absence of legislation, by this bill and chapter 119 of title 18, Congress will have legislated with regard to electronic surveillance in the United States, that legislation with its procedures and safeguards prohibit the President, notwithstanding any inherent powers, from violating the terms of that legislation.

Section 201(c)

This amendment would repeal 18 U.S.C. § 2511(3), which states that nothing in chapter 119 or section 605 of the Communications Act of 1934 shall limit the constitutional power of the President to gather necessary intelligence to protect the national security. In the *Keith* case the Supreme Court held that this section was not a congressional recognition or affirmance of an inherent Presidential power to engage in warrantless surveillance for intelligence purposes to safeguard the national security. Rather, "it merely provided that [chapter 119 and section 605] shall not be interpreted to limit or disturb such power as the President may have under the Constitution. In short, Congress simply left presidential powers where it found them." 407 U.S. at 303. The Foreign Intelligence Surveillance Act, however, does not simply leave Presidential powers where it finds them. To the contrary, this bill would substitute a clear legislative authorization pursuant to statutory, not constitutional, standards. Thus, it is appropriate to repeal this section, which otherwise would suggest that perhaps the statutory standard was not the exclusive authorization for the surveillances in-

cluded therein. Because, however, 18 U.S.C. § 2511(3) was not a recognition or affirmance of presidential power to authorize warrantless surveillances in the absence of legislation, the repeal of this section is equally not a denial of such a power.

Section 201(d)

This amendment makes explicit that the requirements for an application contained in section 2518(1) apply only to surveillance conducted pursuant to chapter 119, since the Foreign Intelligence Surveillance Act of 1978 contains its own requirements.

Section 201(e)

This amendment makes explicit that the necessary elements for an order set forth in section 2518(4) apply only to surveillance conducted pursuant to chapter 119, since the Foreign Intelligence Surveillance Act of 1978 contains its own requirements.

Section 201(f)

This amendment makes explicit that the procedures for disclosure of the court order and accompanying application under section 2518 (9) apply only to surveillance conducted pursuant to chapter 119, since the Foreign Intelligence Surveillance Act of 1978 contains its own requirements.

Section 201(g)

This amendment makes explicit that the provision for a statutory suppression motion contained in section 2518(10) applies only to surveillances conducted pursuant to chapter 119, since the Foreign Intelligence Surveillance Act of 1978 contains its own requirements.

Section 201(h)

This amendment makes explicit that the reporting requirements of the Administrative Office of the U.S. Courts contained in section 2519(3) apply only to surveillance conducted pursuant to chapter 119, since the Foreign Intelligence Surveillance Act of 1978 contains its own requirements.

TITLE III

Title III essentially delays the effective date of the act until 90 days following the designation of the chief judges pursuant to section 103. 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 court. Under H.R. 7308 (as introduced), the 90 days would begin to run after the first judge was appointed. The change is necessary to insure that the necessary security procedures, which must be implemented by the chief judges of the Special Court and the Special Court of Appeals, are in effect when the first applications are submitted.

Committee Position

The Permanent Select Committee on Intelligence, a quorum being present, voted 8–2 to amend H.R. 7308 and report it favorably on May 17, 1978.

Five Year Cost Projection

The Permanent Select Committee on Intelligence has determined that the only costs which will be incurred by the Government in the administration of H.R. 7308 will be appropriate travel and per diem costs for judges of the Special Court and Special Court of Appeals. The committee is unable to estimate what these costs will be, however, although it feels certain that they will be nominal in nature.

Congressional Budget Office Estimate

As of the filing date of this report, the Committee had received no estimate from the Congressional Budget Office pursuant to Section 403 of the Congressional Budget Act. However, the committee notes that the Congressional Budget Office did submit an estimate on S. 1566, the companion Senate measure to H.R. 7308, to the Senate Committee on the Judiciary on October 13, 1977. The conclusion of the Congressional Budget Office on that occasion was that no additional cost to the Government would result from enactment of S. 1566. The committee repeats its earlier statement that the only possible budget impact that it foresees will be in travel and per diem expenses of judges of the Special Court or Special Court of Appeals (institutions not mentioned in S. 1566).

Executive Branch Estimate

The committee has received numerous comments from various Government agencies whose activities would be affected by H.R. 7308. However, the committee has never received any cost estimates from the Government and is therefore unable to compare the Government's costs to its own estimate pursuant to clause 7(a)(2) of rule XIII.

Inflation Impact Statement

The committee has examined H.R. 7308 to determine if there is a possible inflationary impact on the national economy. Consistent with the committee's earlier determinations as to the cost of H.R. 7308 and pursuant to clause 2(l)(4) of rule XI the committee finds that enactment of H.R. 7308 will have no significant effect on the national economy.

Oversight Findings

The committee had not received a report from the Committee on Government Operations pursuant to clause 2(l)(3)(D) of rule XI as of the time of the filing of this report.

Changes in Existing Law

In compliance with subsection (3) of rule XIII of the Rules of the House of Representatives, 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 in italic, and existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

* * * * * * *

TITLE 18—CRIMES AND CRIMINAL PROCEDURE

* * * * * * *

CHAPTER 119—WIRE INTERCEPTION OR INTERCEPTION OR ORAL COMMUNICATIONS

* * * * * * *

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

* * * * * * *

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, is authorized to intercept a wire or oral communication.]

"(*ii*) *Notwithstanding any other law, communication common carriers, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire or oral communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if the common carrier, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—*

"(*1*) *a court order directing such assistance signed by the authorizing judge, or*

"(*2*) *a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,*

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No communication common carrier, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished an order or certification under this subparagraph, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. No cause of action shall lie in any court against any communication common carrier, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of an order or certification under this subparagraph.".

"(*e*) *Notwithstanding any other provision of this title or section 605 or 606 of the Communications Act of 1934, it shall not be unlawful 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 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.*

"(*f*) *Nothing contained in this chapter, or section 605 of the Communications Act of 1934 (47 U.S.C. 605) shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications by a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978; and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of the Act and the interception of domestic wire and oral communications may be conducted.".*

[(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.]

* * * * * * *

§ 2518. 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. Each application shall include the following information:

* * * * * * *

(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 therefor 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.

(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 communications *intercepted pursuant to this chapter*, 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.

* * * * * * *

§ 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 communications *pursuant to this chapter* and the number of orders and extensions granted or denied *pursuant to this chapter* during the preceding calendar year.

* * * * * * *

SUPPLEMENTAL VIEWS OF REPRESENTATIVE ROMANO L. MAZZOLI

In joining the House Intelligence Committee in August of 1977, I did so with full awareness of the difficulty and the magnitude of the task which faced it.

I view the basic mission of our committee as one to reconcile the sometimes competing interests of national security and civil liberties.

Nowhere is this reconciliation more difficult than in the area of foreign intelligence electronic surveillance.

Electronic surveillance, by its very nature, intrudes upon someone's privacy—the basic right to be left alone. At the same time, our Government must necessarily engage in electronic surveillance activities to carry out its foreign intelligence mission.

To maintain a proper balance here, all foreign intelligence electronic surveillance must be conducted pursuant to official authorization and subject to clear and enforceable guidelines.

Our recent history leads to the inescapable conclusion that the executive branch of government cannot be left to police itself in this area. Congress, by statute, must provide the necessary authorizations, and regulations for foreign intelligence electronic surveillance.

In doing so, Congress must be guided by several factors: the basic civil liberties of the people must be protected; the nation's legitimate intelligence activities must not be impeded; the public's confidence in the U.S. intelligence community must be restored; and, individual intelligence agents must be protected from law suits stemming from official duties faithfully performed.

Since H.R. 7308, as reported by the House Intelligence Committee, generally speaks to these factors, I support the measure and urge its prompt passage by the House.

However, I could have supported H.R. 7308 with much more vigor had it provided for an across-the-board judicial warrant for all foreign intelligence electronic surveillance conducted in the United States. This was the way the measure read as it was reported by the Subcommittee on Legislation, on which I am privileged to serve.

However, after thoughtful debate, the full committee redrafted the bill to eliminate the warrant requirement for two classes of electronic surveillance directed at certain foreign powers.

I voted against this change and remain firmly of the opinion that a judicial warrant should be obtained for all foreign intelligence electronic surveillances.

In this position, I share the view of Attorney General Griffin Bell. He states that the warrant process is the traditional means utilized by our legal system to assure citizens that their government adheres to strict legal process when it must engage in intrusive activities.

The judicial warrant process is the legal process most people understand and in which they have confidence.

Of equal importance, it is a process which protects the individual field agent. Too often intelligence agents face "after-the-fact" criminal or civil liability for engaging in activities which apparently were authorized and ordered by their superiors. The result is low morale within the intelligence community and an understandable reluctance to carry out intelligence-related activities.

The committee's decision to provide a narrow exception to the warrant requirement places a field agent in a predicament. The agent must evaluate a superior officer's order to decide whether it is lawful and can be followed without exposing the agent to a lawsuit somewhere down the road.

Only a judicial warrant—issued by a court after a convincing showing of need by the Government—provides the protection needed by the intelligence agent in the field.

Noting these reservations, I reiterate my strong support for H.R. 7308. It evidences the House Intelligence Committee's thoughtful discharge of the delicate task assigned it.

In striking an essentially proper balance between the interests of national security and the privacy rights of individuals, H.R. 7308 demonstrates the mature belief that a democratic government can protect itself from its enemies while at the same time honoring the liberties of its citizens.

ROMANO L. MAZZOLI.

ADDITIONAL VIEWS OF REPRESENTATIVES MORGAN F. MURPHY AND CHARLES ROSE

Though we fully support the committee reported bill, we feel compelled to pen these additional views in order to correct some of the misconceptions contained in the dissenting views of our colleagues.

Nowhere, for instance, is it mentioned in the dissenting views that the Attorney General and the Director of the FBI have not only stated that the committee bill will not impede intelligence collection, but have also noted that the bill will in fact foster necessary intelligence activities and protect intelligence agents in the conduct of their legitimate activities.

Nowhere is it mentioned in the dissenting views that the Attorney General and the Director of the FBI prefer the "criminal standard" of the committee bill over the so-called non-criminal standard that is contained in the McClory substitute.

Nowhere is it mentioned that in a written opinion submitted to the committee the Justice Department concluded that judicial consideration of warrant applications comports fully with the "case of controversy" requirement of article III of the Constitution.

Finally, nowhere is it mentioned that at the present time a civil suit is pending against the Attorney General and several intelligence personnel for activities authorized and conducted under existing executive guidelines, which activities the judge in the *Truong/Humphrey* case found to be unconstitutional because they were not conducted pursuant to a judicial warrant.

When we turn to what is mentioned in the dissenting views, it becomes reasonable to ask if we are commenting on the same bill, testimony and report.

For example, as the majority report notes in detail, the committee bill is not premised on the proposition that the fourth amendment requires a warrant for every search.

Nor did any intelligence community personnel, in either open or closed session, state or imply that a warrant requirement "would pose serious threats to the two most important elements in effective intelligence gathering: (1) speed and (2) security." Indeed, the only intelligence collection activity about which any reservation was expressed has been exempted by the committee bill from a warrant requirement.

Philip Lacovara is cited in the dissenting views as stating that the most effective way of preventing abuses is fixing record responsibility, suggesting that he would support a nonwarrant proposal. In fact, Mr. Lacovara in both his law review article and testimony supported a warrant requirement and specifically opposed a nonwarrant approach. The fixing of record responsibility was only one, and not the most important, reason for his support of a warrant.

The Attorney General is cited as noting that there is substantial question whether the fourth amendment protects foreigners in the

United States. The dissenters ignore the Department of Justice letter written to the committee specifically in response to a question by the committee. That letter unequivocally states that foreigners in the United States are protected by the fourth amendment, if they do not enjoy diplomatic privileges.

The dissenters claim that a steady stream of sensitive information will go to "at least 17 judges (and their clerks, reporters, and bailiffs)." They ignore the fact that the bill specifically provides that court support personnel may be provided by the Executive, as the Supreme Court suggested in *Keith*. They ignore the fact that an application is made to only 1 judge, not to 17, and that 6 of the 17 judges are on the Special Court of Appeals. They also ignore the parallel experience in the law enforcement field where, over a period of 10 years, no wiretap application has ever been appealed.

Finally, the dissenters refer to the bill as having an across-the-board warrant requirement. They ignore the fact that the bill specifically authorizes the most sensitive class of surveillances without a warrant requirement and specifically provides for warrantless emergency surveillances where there is insufficient time to get to the court (so much for the alleged threat to security posed by the need for speed). And nowhere do the dissenters acknowledge that only where U.S. citizens may be involved is a warrant required by the bill.

One unassailable point emerges from the committee's consideration of H.R. 7308: Every intelligence community witness that has testified before this committee supports passage of the committee reported bill.

MORGAN F. MURPHY.
CHARLIE ROSE.

DISSENTING VIEWS ON H.R. 7308

> The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports are not and ought not to be published to world. It would be intolerable that courts, without the relevant information, should review and perhaps nullify actions of the Executive taken on information properly held secret. Nor can courts sit in camera in order to be taken into executive confidences. But even if courts could require full disclosure, the very nature of executive decisions as to foreign policy is political, not judicial. Such decisions are wholly confided by our Constitution to the political departments of the government, Executive and Legislative. They are delicate, complex, and involve large elements of prophecy. They are and should be undertaken only by those directly responsible to the people whose welfare they advance or imperil. They are decisions of a kind for which the Judiciary has neither aptitude, facilities nor responsibility and which has long been held to belong in the domain of political power not subject to judicial intrusion or inquiry.

These words are as true today as they were when Justice Jackson wrote them for the Supreme Court in 1948.[1] Unfortunately, the committee ignored this lesson in constitutional law. By requiring a judicial warrant to authorize the use of electronic surveillance to gather foreign intelligence information, H.R. 7308 would thrust the judicial branch into the arena of foreign affairs and thereby improperly subject "political" decisions to "judicial intrusion."

No one can deny that abuses of electronic surveillance have taken place in the past under the claim of "national security." The action taken by the committee to amend and then approve H.R. 7308 is intended as an answer to those abuses. But, it ignores the experience of the past few years under Executive orders issued by Presidents Ford and Carter. These guidelines were designed to regulate the use of electronic surveillance for foreign intelligence purposes, and all of the evidence received by the committee indicates that they have served their purpose of making this method of intelligence gathering abuse-free.

The committee bill would pack up all of the problems involved in this sensitive and complex area of foreign intelligence electronic surveillance and ship them to a specially established Federal court. Here are some of the things H.R. 7308 would do:

---

[1] *Chicago & Southern Air Lines, Inc.* v. *Waterman Steamship Corp.*, 333 U.S. 103, 111 (1948) (citations omitted).

It would give to a single judge the power to deny the President the use of electronic surveillance of an individual—despite the fact that the court may have found the individual to be a spy working for a foreign government against the interests of the United States. [2]

It would give to a single judge the authority and responsibility to order (or refuse to order) our intelligence agencies to engage in foreign intelligence electronic surveillance—despite the fact that all of the court decisions which have dealt with the issue clearly establish that the fourth amendment does not require a judicial warrant to authorize surveillance of foreign powers or their agents. [3]

Finally, it would give to a special court the primary responsibility of oversight of the executive branch's use of electronic surveillance for foreign intelligence purposes—despite the fact that the Constitution reposes such responsibility in the Congress. [4]

This is not simply a case of overkill. It is—in addition—as former Deputy Attorney General Laurence Silberman declared before the committee's Legislation Subcommittee, "an enormous and fundamental mistake which the Congress and the American people would have reason to regret." [5]

Because our Government needs accurate information to protect our country from the hostile acts of foreign powers, it is necessary to engage in electronic surveillance of the agents of such powers. This is true if the agents are foreigners, as well as in the rare situation that a traitorous American citizen is working clandestinely for a foreign power. It would plainly be inappropriate to go beyond the fourth amendment mandate by requiring a warrant to authorize such activities, for as Judge Bryan stated in his recent opinion in the *Humphrey/Troung* espionage case:

> It is not at all certain that a judicial officer, even an extremely well-informed one, would be in a position to evaluate the threat posed by certain actions undertaken on behalf of or in collaboration with a foreign state . . . The Court is persuaded that an initial warrant requirement [for foreign intelligence electronic surveillance] would frustrate the President's ability to conduct foreign affairs in a manner that best protects the security of our government.[6]

THREAT TO NATIONAL SECURITY

It is contended that nothing in the judicial warrant procedure in this bill threatens the national security. For support, it is noted that

[2] If the proposed surveillance target is a U.S. citizen or permanent resident alien, a senior executive branch official must certify that the information sought is "necessary" to certain defined security or foreign policy interests of the United States. Even after finding the target to be working clandestinely for a foreign power, the court can deny an application for authorization of surveillance if it finds that the information is not "necessary."

[3] *United States* v. *Buck*, 548 F.2d 871 (9th Cir. 1977); *United States* v. *Butenko*, 494 F.2d 871 (3rd Cir. 1974) (en banc), cert. den. sub nom., *Ivanov* v. *United States*, 419 U.S. 881 (1974); *United States* v. *Brown*, 484 F.2d 418 (5th Cir. 1973), cert. den., 415 U.S. 960 (1974); *United States* v. *Humphrey and Troung*, Crim. No. 78–25–A (E.D. Va., mem. opinion March 30, 1978).

[4] H.R. 7308, Section 105(d).

[5] Hearings before the Subcommittee on Legislation of the House Permanent Select Committee on Intelligence, Hearings on the Foreign Intelligence Electronic Surveillance Bills, 95th Cong., 2d Sess. (1978) [hereinafter. Hearings].

[6] *United States* v. *Humphrey and Troung*, Crim. No. 78–25–A (E.D.Va., mem. opinion March 30, 1978). The defendants were convicted in a jury trial on May 19, 1978 on espionage and other charges.

no administration official testified that the bill would frustrate our intelligence-gathering operations.

These senior members of the intelligence community were testifying publicly on H.R. 7308 as introduced—that is, to a bill that required a a judicially-authorized warrant in all cases. They were carrying the administration banner in full support of the bill.

However, as time went on some administration officials broke ranks to support an exception to the across-the-board warrant requirement. Despite strong pressures from administration leaders outside of the intelligence community, these highly knowledgeable operating intelligence personnel conceded that a warrant requirement, by mandating prior disclosure to judges of the most sensitive intelligence information, would pose serious threats to the two most important elements in effective intelligence gathering: (1) speed and (2) security.

The real possibilities of delay and disclosure of classified information are risks the intelligence community should not be required to take. For example, the threat of disclosure is obvious when it is remembered that H.R. 7308 requires that a steady stream of extremely sensitive written information flow to at least 17 judges (and their clerks, reporters, and bailiffs), all of whom are ill-equipped to provide the required security procedures. Clearly, the more people who become involved in intelligence activities, the greater the risk of disclosure. As the Director of Central Intelligence, Adm. Stansfield Turner, has often indicated:

> Minimizing the number of people who have to have access to this information is a basic security principle.[7]

In short, the committee bill represents the very kind of interference with Executive authority that frustrates effective foreign policy and national security actions by a responsible chief executive.

Fortunately, the committee took heed of these warnings and adopted an amendment, offered by Mr. McClory, which exempted certain highly technical surveillance activities from the warrant requirement.[8]

Without the pressures which were applied, we are confident that these same officials would have candidly expressed other reservations about the legislation. Suffice it to say that many in the intelligence community regard this bill as a serious threat to our country's national security by opening to compromise the security of our intelligence-gathering operations.

THE CONSTITUTION AND FOREIGN INTELLIGENCE GATHERING

Article II of the Constitution provides that the President shall "preserve, protect and defend the Constitution of the United States." [9] He is he Commander-in-Chief of the Armed Forces of this country and has primary responsibility for the conduct of our foreign affairs. In the execution of these duties, and as head of state, he therefore exercises powers to protect the national security.

Among such powers is the power to authorize intelligence-gathering activities aimed at efforts of foreign governments or their agents which

[7] Hearings.

[8] This was referred to as McClory Amendment IX.

[9] Article II, Section 1, clause 7.

are inimical to the security of the United States. While statutory regulation of this technique seems proper, it is clearly inappropriate to inject the Judiciary into this realm of foreign affairs and national defense which is constitutionally delegated to the President and to the Congress.

The committee bill rests on the proposition that the fourth amendment to the Constitution presumptively requires a warrant for every search, and particularly electronic searches because of their sweeping character. The underlying reasoning for this assertion was that in view of the Supreme Court's decision in the *Keith* [10] case (which ruled that a warrant is required for electronic surveillances employed for domestic security purposes—that is, where no involvement of a foreign power is shown), it would be appropriate to require a warrant for foreign intelligence purposes.

Such an argument overlooks the clear reservation in *Keith* that the court was in no way addressing the issues involved in foreign intelligence electronic surveillance.[11] This argument also ignores the weight of circuit court cases upholding the inherent constitutional right of the President to authorize warrantless electronic searches for foreign intelligence purposes. Just last year, the ninth circuit declared, "Foreign security wiretaps are a recognized exception to the general warrant requirement [of the fourth amendment]." [12]

It should be noted that the only strong support for the argument that the fourth amendment mandated a warrant in the area of foreign intelligence gathering came from the bill's strongest proponent—the American Civil Liberties Union (ACLU). Actually, the ACLU contends that even with a warrant there is inadequate protection of privacy, urging that all electronic surveillance—for whatever purpose—is unconstitutional in that it violates the fourth amendment.

Let us hope that no judge ever agrees with that position. But, if only one judge of the special court established by this bill should so find, he could for an uncertain and critical period virtually paralyze vital intelligence-gathering activities.

Most of those who testified before the subcommittee—even proponents of the bill's warrant provision—argued that a warrant is not constitutionally required. This, indeed, is the very position put forward by the Justice Department, and sustained by the court, in the *Humphrey/Troung* case.

In this regard, it is interesting, and somewhat ironic, that the Attorney General now voices strong support for the bill's warrant provision. When sitting on the Fifth Circuit Court of Appeals, Judge Bell expressed, in *United States* v. *Brown*, a diametrically opposite view:

> In *United States* v. *Clay*, the case referred to in the Supreme Court's footnote 20 [to the *Keith* case], we concluded that the President had [the authority to engage in foreign intelligence electronic surveillance] over and above the Warrant Clause of the Fourth Amendment.

[10] *United States* v. *United States District Court*, 407 U.S. 297 (1972). The Honorable Damon J. Keith, of the Eastern District of Michigan, was the district judge whose orders the government was challenging.
[11] 407 U.S. at 308, 321–22.
[12] *United States* v. *Buck*, 548 F. 2d 871, 875 (9th Cir. 1977). See cases cited, supra, note 3.

> We found that authority in the inherent power of the President with respect to conducting foreign affairs. We took our text from *Chicago & Southern Air Lines* v. *Waterman S.S. Corp.*, where the Supreme Court stated:
> "[T]he President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports are not and ought not to be published to the world. *It would be intolerable that courts, without the relevant information, should review and perhaps nullify actions of the Executive taken on information properly held secret.*"
>
> * * * * * * *
>
> As [the *Keith* case] teaches, in the area of domestic security, the President may not authorize electronic surveillance without some form of prior judicial approval. However, because of the President's constitutional duty to act for the United States in the field of foreign relations, *and his inherent power to protect national security in the context of foreign affairs*, we reaffirm what we held in United States v. Clay, *supra*, that *the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence.*
> Our holding in *Clay* is buttressed by a thread which runs through the Federalist Papers: that the President must take care to safeguard the Nation from possible foreign encroachment, whether in its existence as a nation or in its intercourse with other nations.[13]

Because the Constitution does not demand a warrant in this area, the issue as to whether or not a warrant should be required presents a question of policy. The policy called for is the one which will best serve the interests of the American people, for these are the people referred to in the Preamble to our Constitution—"We the people . . ."—and in the fourth amendment—"The Right of the People to be secure . . . against unreasonable Searches and Seizures shall not be violated." Yet, as the Attorney General has publicly indicated, based on existing guidelines during the past 18 months only one American citizen [14] has been subject to electronic surveillance. Therefore, from a practical standpoint, by enacting the administration bill, we would be establishing a cumbersome procedure involving the unprecedented injection of judicial discretion into foreign intelligence decision-making, all to add incrementally, if at all, to the protections which already exist.

Judicial authorization of electronic surveillance for national security purposes poses another constitutional question: There is serious doubt as to whether the Constitution even permits judicial consideration of such warrant applications as H.R. 7308 contemplates, for article III limits Federal courts to "cases" and "controversies."

This requirement is clearly met in situations where the government contemplates prosecution. Where this is unlikely at all—and where

[13] *United States* v. *Brown*, 484 F. 2d 418, 426 (5th Cir. 1973), cert. den., 415 U.S. 960 (1974) (citations omitted) (emphasis added).
[14] Ronald Louis Humphrey. See *United States* v. *Humphrey and Troung*, supra, note 6.

Presidential conduct of foreign affairs is involved—it becomes a very real question as to whether any case will ever develop for a court to hear. There might never be an adversary proceeding in which the Judiciary could play its impartial role. Rather, by involvement in the authorization process of foreign intelligence gathering by electronic surveillance, judges can actually become involved in the operation of intelligence activities. It will likely be rarely considered that an adversary hearing is the inevitable result of electronic surveillance under H.R. 7308. Dictates of security have always (with only one exception) [15] militated against prosecutions in the past. Based on this experience, it requires a severe straining of Article III to view the activities which the bill seeks to authorize as constitutionally sufficient to allow judicial involvement.

MORE REASONS WHY JUDICIAL INVOLVEMENT IS WRONG

In addition to the constitutional provisions which, we believe, allow for warrantless electronic surveillance for foreign intelligence purposes, there are substantial practical and policy considerations which militate against involving the Judiciary in foreign intelligence matters of this kind.

To begin with, Federal judges are for the most part unequipped, either by training or experience, to make the subtle political and operational decisions that must be made daily by intelligence personnel. Judges are simply not selected in order that they might pass on the merits of foreign intelligence gathering just as they are not called upon to draft treaties or negotiate trade agreements—and this is how it should be.

To say that the judges will be engaged solely in the normal judicial role of applying statutory criteria to a set of facts is to beg the question, for the criteria themselves involve intelligence-related judgments. As pointed out by Laurence Silberman in his testimony before the Subcommittee on Legislation:

> The scope of judicial review for targeted United States persons under the Administration bill clearly propels the judiciary into policy determinations of breathtaking scope.[16]

For example, in reviewing the certification that the information sought is foreign intelligence information under the "clearly erroneous" standard,[17] the judge must consider what information "is necessary to the ability of the United States to protect against actual or potential attack or other grave hostile acts," [18] and what information with respect to a foreign power "is necessary to the national defense" [19] or the successful "conduct of foreign affairs." [20]

Finally, even if the bill does carefully establish strict guidelines for the special court to follow, judges apparently cannot be compelled to limit their roles within legislative restraints. One need only note recent

[15] *United States* v. *Humphrey and Troung*, supra, note 6.
[16] Hearings.
[17] H.R. 7308, Section 105(a)(5).
[18] H.R. 7308, Section 101(e)(1).
[19] H.R. 7308, Section 101(3)(2)(A).
[20] H.R. 7308, Section 101(e)(2)(B).

court decisions in the field of environmental law to find support for this assertion. Likewse, let there be no question in anyone's mind that judges, if assigned the prerogatives in the committee bill, will undertake and expand upon any such role granted to them by this legislation.

CONGRESSIONAL OVERSIGHT

The use of electronic surveillance to gather foreign intelligence information is important to our relations with foreign governments. As it effects the conduct of our foreign affairs it can be seen to involve political decisions. These decisions—in the first instance—are properly made by the Executive. But history shows that the Executive cannot be given unbridled discretion in directing intelligence activities. Thus comes into play the need for congressional oversight.

It is the Congress which can best assure the proper functioning—without abuse—of our intelligence gathering operations by exercising its constitutionally assigned role of a political check on the Executive. Aggressive oversight will let the Executive know that, should abuses occur, they will not go undiscovered, undisclosed, or unpunished. Indeed, the reason that select committees on intelligence were established in both Houses was to facilitate effective congressional oversight of intelligence community operations.

H.R. 7308 would not only require a judge to give prior judicial sanction to each use of foreign intelligence electronic surveillance, but it also would empower the court to look into the day-to-day operations of this activity.[21] After the warrant was issued, the court would be allowed to gain access to *all* information obtained by the surveillance to see that intelligence personnel did not improperly obtain, use, or disseminate such information.

By giving the primary oversight function to a special court, Congress could easily be lulled into laziness, feeling that the court was adequately reviewing the situation. But the judges of this court—who each will only be serving perhaps one or two months out of the year—will be ill-equipped to meet the task.

The operations, in total secrecy, of 17 judges who are politically unresponsive to the American people can do little to further the goal of restoring public trust in our intelligence agencies. This is a job requiring the resources—and the political sensitivity and accountability—of the Congress.

THE "CRIMINAL STANDARD"

Beyond the obvious folly of vesting broad powers in judges who may thereby consider themselves qualified to second guess both the President and his Cabinet officers, the bill would open a Pandora's box of other issues.

One such issue created by H.R. 7308, as amended by the committee, would be involved where the person to be targeted for foreign intelligence electronic survellance is a "United States person." In such cases the court may approve such surveillance only where the person targeted may be involved in some criminal activity. The concept that

[21] H.R. 7308, Section 105(d).

national security electronic surveillance must be linked to a criminal standard is nowhere to be found in the Constitution.[22] The fourth amendment provides protection against unreasonable searches and seizures. When the government seeks evidence to support a prosecution, it may be reasonable to require that the probable cause standard apply to the issue of criminality itself. Where, however, the object of the government is to gather intelligence relating to national security or defense of the country, the situation is very different.

Whether the activities which the President may wish to scrutinize are illegal or not is not of primary importance, for the government does not seek the information to prosecute. While prosecution may prove to be a viable option, the main thrust of our efforts in this area are to protect against foreign intelligence activities which threaten our security. Prosecution may be, as most often has been the case, inappropriate or harmful to that effort. To impose a criminal standard, therefore, adds a requirement, not mandated by the Constitution, which could in fact inhibit powers reserved to the Executive.[23]

FIXING RECORD RESPONSIBILITY IS KEY TO PREVENTING ABUSE

A primary lesson that has been learned from the disclosures of abuses by past administrations is the need to insure high level executive branch responsibility and accountability for particular actions taken in the name of national security. Yet, H.R. 7308, as amended, will surely have the opposite effect.

It should be seen that by shifting from the President to the judiciary the responsibility to authorize foreign intelligence electronic surveillance, the courts become a buffer to Executive accountability. The decision as to whether a surveillance may be undertaken will be the judge's, not the President's. If an intelligence agency wants to use electronic surveillance for an improper purpose, an application can be made to a court for authorization. In this secret proceeding the strongest response a judge can make to the application is to deny it. But, it appears inevitable that some judges—perhaps by granting too much deference to the intelligence community—might give approval to abusive actions. In the face of an abusive surveillance, the Executive would be able to wash its hands of the whole matter by passing the buck to the judge that approved it. Furthermore, knowing that responsibility for the final decision rests elsewhere, government officials would be inclined to refer all doubtful or particularly difficult cases to the judge.

It is even more likely that executive branch scrutiny will wane over time if, as proponents of the warrant requirement concede, applications for warrants will be rarely, if ever, denied. If such a "rubber stamp" procedure is the likely result, it is difficult to perceive how the American people will thereby regain confidence in our intelligence agencies.

[22] Even the plurality opinion in *Zweibon* v. *Mitchell*, 516 F. 2d 594 (D.C. Cir. 1975)—which held that a warrant is required in domestic security cases, and which in dicta indicated that the fourth amendment mandates a warrant for all electronic surveillances—found no need for a criminal standard.

[23] To mandate a judicial finding of criminal conduct before a warrant may be issued to search for foreign intelligence information can be seen as particularly onerous in light of the recent Supreme Court decision in *Zurcher* v. *Stanford Daily*, 46 USLW 4546 (May 31, 1978). There, the Court held 5–3 that in a law enforcement context—where one might expect the restrictions on government actions to be greater than in foreign intelligence matters—a search warrant may properly be issued to obtain information even from a totally innocent person if there is probable cause to believe that such information relates to a criminal violation.

See also Marshall v. *Barlow's, Inc.*, 46 USLW 4483 (May 23, 1978), a case striking down warrantless OSHA searches, in which the Court held that fourth amendment warrants may be issued without a probable cause determination that a crime has been committed.

As former Solicitor General and Acting Attorney General Robert Bork, now a Yale law professor, commented:

> When an Attorney General must decide for himself, without the shield of a warrant, whether to authorize surveillance, and must accept the consequences if things go wrong, there is likely to be more care taken. The [Administration bill], however, has the effect of immunizing everyone, and sooner or later that fact will be taken advantage of. It would not be the first time a regulatory scheme turned out to benefit the regulated rather than the public.[24]

Under the current guidelines of Executive Order 12036, it is the Attorney General who individually passes judgment on each use of foreign intelligence electronic surveillance. It is unpersuasive, indeed, for the Attorney General to seek to renounce a responsibility he now has by urging that a special court should make decisions *for him* when foreign intelligence surveillance is needed in behalf of our country's national security.

AN ALTERNATE PROPOSAL

In reviewing the abuses of the past, it can be seen that the method used by senior executive branch officials to try to escape responsibility was by establishing "plausible deniability." As noted by Philip Lacovara, the former Counsel to Watergate Special Prosecutors Archibald Cox and Leon Jaworski, the most effective way to prevent these abuses would be to fix record responsibility on those who authorize foreign intelligence electronic surveillance.[25]

It appears doubtful that anyone would abuse this authority if a statute provided that:

(1) all authorizations of surveillance be made in writing.

(2) all written records be maintained and be subject to later inspection by the duly constituted House and Senate intelligence committees.

(3) any abuse would subject the guilty party to civil and criminal liability.

This three-part solution represents the foundation for the substitute measure offered in the committee by Congressman McClory. The McClory substitute would strike the most realistic balance between our necessary foreign intelligence and national security needs and the liberties which are bound to defend through such activities. It would retain within the Executive—where it should be—the authority to approve foreign intelligence electronic surveillance. Such activities would require the approval in writing of the Attorney General and a confirmed senior executive branch official. In addition, when the target is an American citizen, the President's approval would also be needed. These duties would be nondelegable. By requiring the con-

[24] "Reforming Foreign Intelligence," Wall Street Journal, March 19, 1978.

[25] Lacovara, "Presidential Power to Gather Intelligence," 40 Law & Contemporary Prob. 106 (1976); Hearings.

sensus of the President and the two highest national security officials to approve a surveillance, it is clear that the proposed statutory authority would only be used when truly required by the national interest. Furthermore, such a consensus requirement would provide a true measure of Executive accountability.

Some who support the committee's bill assert that only a law mandating a warrant will put to rest the concerns over fourth amendment requirements. This is nonsense. All of the witnesses heard by the subcommittee who addressed the McClory substitute—including those who favor a warrant provision—attest to its constitutionality. Even Morton Halperin, who strongly aligns himself with the ACLU, so testified:

> I think it is also clear that [the McClory bill] would make it much more likely that the courts would accept warrantless wiretaps because they would then be done on the basis of both Congressional and Executive Branch authorization.[26]

Clearly, the McClory substitute would pass constitutional muster.

Those who prefer H.R. 7308 to the substitute also argue that while the former would prevent abuses by interposing the judiciary between the expressed desire to engage in surveillance itself, the substitute would provide only an after-the-fact discovery mechanism. This analysis is patently erroneous. The substitute bill would establish strict statutory guidelines—with civil and criminal penalties for their violation—along with the requirement that authorizations be made in writing. Thus, the substitute would provide a completely adequate deterrance to abuse.

No matter what the law, if an executive branch official chooses to engage in abusive electronic surveillance, he need only ignore the statutory requirements, whatever they may be. However, under the provisions of either H.R. 7308 or the substitute, ignoring the statute would be a criminal violation.

With this in mind, it can be seen that the McClory substitute providing for oversight by the House and Senate Intelligence Committees represents a sufficient statutory solution to a complex problem. This being so, there appears to be no compelling reason to go further by providing for a judicial role in intelligence matters, especially when to do so is historically unprecedented and constitutionally suspect.

Assuming, *arguendo*, that a judicial warrant for foreign intelligence electronic surveillance will somehow act as a talisman under which abuses and the doubts of the American people will disappear, it is nevertheless suggested that the across-the-board warrant requirement of H.R. 7308 is unnecessary and unwise. If at all justified, it is only so where U.S. citizens are involved. Perhaps, in this limited area, the sense of protection of civil liberties perceived to be gained by a warrant requirement would outweigh the many ill effects that would result therefrom. However, it is unlikely that foreign embassies, governments, or visitors have a legitimate or reasonable expectation of privacy under the fourth amendment or that the American people are demanding that our intelligence agencies provide more protection to

[26] Hearings.

foreign agents. As Attorney General Bell noted in his testimony before the Subcommittee on Legislation, there is substantial doubt as to whether the fourth amendment applies to foreigners and their governments.[27] And, even if it does apply, it is certainly "reasonable"—as the fourth amendment requires—for the President to order surveillance of foreigners and foreign embassies without judicial approval.

While the committee did not adopt this view, it must be noted that a compromise amendment that would have extended the warrant only to United States persons failed on a six-to-six tie vote.[28] Therefore, any assertion that the committee overwhelmingly supports the across-the-board warrant provision of H.R. 7308 is quite incorrect—and misleading.

CONCLUSION

If President Carter feels that the Congress has already tied his hands in such a manner as to thwart his conduct of foreign affairs—he should be doubly apprehensive of this measure (H.R. 7308) under which the Congress could well frustrate his ability to secure, by electronic means, foreign intelligence essential to the protection of our national security. We urge the rejection of H.R. 7308 and the approval of an amendment in the nature of a substitute which will be offered by Congressman McClory.

Bob Wilson.
Robert McClory.
J. Kenneth Robinson.
John M. Ashbrook.

[27] Hearings.
[28] This was referred to as McClory Amendment II.

○