Calendar No. 643

95TH CONGRESS
2D SESSION

SENATE

REPORT
No. 95-701

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

MARCH 14, (legislative day, FEBRUARY 6), 1978.—Ordered to be printed

Mr. BAYH, from the Select Committee on Intelligence, submitted the following

REPORT

together with

ADDITIONAL VIEWS

[To accompany S. 1566]

The Select Committee on Intelligence, to which was referred the bill (S. 1566) to amend title 18, United States Code, to authorize applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information, having considered the same, reports favorably thereon with amendments and recommends that the bill, as amended, do pass.

AMENDMENTS

On page 1, line 4, strike "1977", and insert in lieu thereof "1978".

On page 3, strike out all after line 5 through the end of line 19, and insert in lieu thereof the following:

(A) any person, other than a United States person, who—

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

(ii) acts for or on behalf of a foreign power which engages in clandestine intelligence activities 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 conspires with any person knowing that such person is engaged in such activities;

On page 3, strike out all after line 19 through line 23 on page 4, and insert in lieu thereof the following:

(B) any person who—

(i) 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;

(ii) 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;

(iii) knowingly engages in sabotage or terrorism, or activities which are or may be in preparation therefor, for or on behalf of a foreign power;

(iv) knowingly aids or abets any person in the conduct of activities described in subparagraph (B) (i) through (iii) above, or conspires with any person knowing that such person is engaged in activities described in subparagraph (B) (i) through (iii) above: *Provided*, That no United States person may be considered an agent of a foreign power solely upon the basis of activities protected by the First Amendment to the Constitution of the United States.

On page 5, strike out all after line 14 through line 15 on page 6, and insert in lieu thereof:

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

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

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

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

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

(i) sabotage or terrorism by a foreign power or an agent of a foreign power, or

(ii) the clandestine intelligence activities of an intelligence service or network of a foreign power or an agent of a foreign power.

On page 8, line 8, strike the first comma and insert in lieu thereof the word "and".

On page 9, strike out all after line 2 through line 22, and insert in lieu thereof the following:

> and which are reasonably designed to insure that information which relates solely to the ability of the United States to provide for the national defense or security of the Nation and to provide for the conduct of the foreign affairs of the United States, under subparagraphs (B) and (C) above, shall not be disseminated in a manner which identifies any United States person, without such person's consent, unless such person's identity is necessary to understand or assess the importance of information with respect to a foreign power or foreign territory or such information is otherwise publicly available.

On page 10, line 6, after the word "powers", insert the following: "as defined in section 2521 (b) (1) (A)-(E)."

On page 10, line 25, strike the words "each of whom," and insert in lieu thereof the following: "who shall constitute a special court, each member of which".

On page 12, insert after line 8 a new subsection as follows:

> (d) Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, provided that the judges first designated under subsection (a) shall be designated for terms of from one to seven years so that one term expires each year, and that judges first designated under subsection (b) shall be designated for terms of three, five, and seven years.

On page 12, strike lines 23 and 24, and insert in lieu thereof the following:

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

On page 17, line 6, after the letter "(E)", insert the following: "and any other information furnished under section 2524(c)".

On page 20, line 2, after the word "cause.", insert the following new sentence: "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 required by this chapter."

On page 21, line 13, after the word "thereof", insert the following:

> ; 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 where the information indicates a threat of death or serious bodily harm to any person.

On page 21, line 22, after the letter "(F)", insert the following: "and in accordance with the minimization procedures required by this chapter,".

On page 22, line 12, after the word "Government," insert the following: "of the United States, of a State, or of a political subdivision thereof".

On page 26, insert after line 14 a new subsection as follows:

(g) 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 where both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, except with the approval of the Attorney General where the contents indicate a threat of death or serious bodily harm to any person.

On page 26, insert after line 24 a new section as follows:

§ 2528. Congressional Oversight.

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

(b) On or before one year after the effective date of this chapter, and on the same day each year thereafter, the Select Committee on Intelligance of the United States Senate shall report to the Senate concerning the implementation of this chapter. Said reports shall include but not be limited to an analysis and recommendations concerning whether this chapter should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment.

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

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

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

(f) In the case of any disagreement between the two Houses of Congress with respect to such legislation passed

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

On page 29, line 17, after the number "2520.", insert the following new sentence:

No communication common carrier of officer, employee or agent thereof shall disclose the existence of any interception under this chapter or electronic surveillance, as defined in chapter 120, with respect to which the common carrier has been furnished either an order or certification under this subparagraph, except as may otherwise be lawfully ordered.

On page 30, line 8, after the word "duty," insert the following: "under procedures approved by the Attorney General".

On page 31, line 2, after the word "provided," insert the following: "that no particular United States person shall be intentionally targeted for such purposes without his consent,".

On page 31, line 13, after the word "international," insert the words "or foreign".

Purpose of Amendments

The Committee on the Judiciary adopted several amendments to S. 1566 designed to clarify and make more explicit the statutory intent, to provide further safeguards for individuals subjected to electronic surveillance pursuant to this new chapter, and to provide a detailed procedure for challenging such surveillance, and any evidence derived therefrom, during the course of a formal proceeding.

The purpose of the amendments adopted by the Select Committee on Intelligence has been to clarify further the legislative intent and to provide additional safeguards for persons who may be subjected to electronic surveillance, including a criminal standard for surveillance of U.S. citizens and resident aliens. Judicial procedures for issuing court orders for foreign intelligence surveillance, as well as for monitoring compliance with such orders, are described in greater detail. An effort has also been made to strengthen protection against abuses involving dissemination and use of information received through such surveillance. Specific provisions requiring regular congressional oversight have been added.

Finally, the reported bill adds amendments to chapter 119 of title 18, United States Code (title III of the Omnibus Crime Control and Safe Streets Act of 1968, Public Law 90–351, section 802). These amendments are technical and conforming in nature and are designed to integrate certain provisions of chapters 119 and 120. A more detailed explanation of the individual amendments is contained in the section-by-section analysis of this report.

History of the Bill

The Foreign Intelligence Surveillance Act of 1977, S. 1566, was introduced by Senator Kennedy on May 18, 1977 to provide a statutory procedure to authorize applications for a court order approving the use of electronic surveillance within the United States to obtain foreign intelligence information. The bill, cosponsored by seven other Senators (Mr. Bayh, Mr. Eastland, Mr. Inouye, Mr. McClellan, Mr. Mathias, Mr. Nelson, and Mr. Thurmond), was referred to and considered by the Committee on the Judiciary. That committee reported the bill favorably on November 15, 1977; and it was referred to the Select Committee on Intelligence.

S. 1566 has its origin in S. 3197, The Foreign Intelligence Surveillance Act of 1976, 94th Congress, second session (1976). That legislation, also introduced by Senator Kennedy, had the same broad, bipartisan support, including that of the Ford administration, as S. 1566 and was the subject of Senate hearings by both the Subcommittee on Criminal Laws and Procedures of the Committee on the Judiciary and the Select Committee on Intelligence, S. 3197 was reported favorably by both Senate committees by a combined vote of 24 ayes and 2 nays, but the session ended before the full Senate could act on the legislation.

S. 1566 picks up where S. 3197 left off. Hearings were held by the Subcommittee on Criminal Laws and Procedures, chaired by Senator Kennedy at the request of Senator McClellan. Hearings were also held by the Subcommittee on Intelligence and the Rights of Americans, chaired by Senator Bayh, and included executive session hearings to consider classified information bearing upon the bill. Among those testifying before one or both of these subcommittees were Attorney General Griffin B. Bell; Director of the FBI Clarence M. Kelley; Director of Central Intelligence Stansfield Turner; Secretary of Defense Harold Brown; John Shattuck and Jerry Berman of the American Civil Liberties Union; Morton H. Halperin of the Center for National Security Studies; Steven Rosenfeld of the Committee on Federal Legislation of the Association of the Bar of the city of New York; and David Watters of the American Privacy Foundation.

Broad-based support was voiced for S. 1566 throughout the hearings, with the administration indicating its support of the bill.

S. 1566 as reported has been amended in several respects to respond to the constructive criticisms and suggestions elicited in the hearings. As amended, the bill was approved by the Select Committee on Intelligence, 15–0, with a recommendation for favorable action.

Position of the Administration

The administration has supported the enactment of S. 1566 and supports its swift passage by the Senate. As Attorney General Bell stated in testifying in favor of the bill:

> I believe this bill is remarkable not only in the way it has been developed, but also in the fact that for the first time in our society the clandestine intelligence activities of our Government shall be subject to the regulation and receive the posi-

tive authority of a public law for all to inspect. President Carter stated it very well in announcing this bill when he said that "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, and a balance which cannot be achieved by sacrificing either our Nation's security or our civil liberties. In my view this bill strikes the balance, sacrifices neither our security nor our civil liberties, and assures that the abuses of the past will remain in the past and that the dedicated and patriotic men and women who serve this country in intelligence positions, often under substantial hardships and even danger, will have the affirmation of Congress that their activities are proper and necessary.[1]

General Statement

I. SUMMARY OF THE LEGISLATION

S. 1566 amends title 18, United States Code, by adding after chapter 119 a new chapter 120 entitled "Electronic Surveillance Within the United States for Foreign Intelligence Purposes." The bill requires a court order for electronic surveillance as defined therein conducted for foreign intelligence purposes within the United States or targeted against the international comunications of particular U.S. persons who are in the United States. The bill establishes the exclusive means by which such surveillance may be conducted. S. 1566 does not require a court order for electronic surveillance abroad, and the bill does not address the question whether the President has any constitutional power to conduct electronic surveillance of a U.S. person abroad without a court order to acquire foreign intelligence information, if such power exists.[2]

Under S. 1566 the Attorney General, upon the general authorization of the President for the conduct of electronic surveillance within the United States for foreign intelligence purposes, may authorize applications to members of a special court for orders to conduct such surveillance. Applications are to be made to one of seven district judges publicly designated by the Chief Justice of the United States to serve staggered 7-year terms on a special court. Denials of such applications may be appealed to a special three-judge court of review and ultimately to the Supreme Court.

Approval of an application under the bill would require a finding by the court that the target of the surveillance is a "foreign power" or an "agent of a foreign power" and that the facilities or place at which the

---

[1] Hearing before the Subcommittee on Criminal Laws and Procedures of the Senate Committee on the Judiciary, Foreign Intelligence Surveillance Act of 1977, 95th Cong., 1st sess., p. 13 (1977).

[2] Further legislation may be needed to protect the rights of Americans abroad from improper electronic surveillance by their Government. Such legislation should be considered separately because the issues are different than those posed by electronic surveillance within the United States. S. 2525, the National Intelligence Reorganization and Reform Act of 1978, has been introduced by members of the Select Committee on Intelligence to fill this gap. Title III of that bill would establish procedures for electronic surveillance of Americans abroad.

surveillance is to be directed are being used or are about to be used by a foreign power or an agent of a foreign power. A "foreign power" may include a foreign government, a faction of a foreign government, a foreign-based terrorist group, a foreign-based political organization, or an entity directed and controlled by a foreign government. An "agent of a foreign power" includes non-resident aliens who act as officers or employees of foreign powers or who act on behalf of foreign powers which engage in clandestine intelligence activities 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 and retention, and prohibit the dissemination, of information concerning U.S. persons which does not relate to national defense, foreign affairs, or the terrorist, sabotage, or clandestine intelligence activities of a foreign power. Additional limits are placed on the dissemination of information relating solely to national defense or foreign affairs.

Finally, a certification or certifications must be 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 successful 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 surveillance of a U.S. person and to determine that the certification is not clearly erroneous.

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.

Emergency surveillance without a court order would be permitted in limited circumstances, but a court order must be obtained within 24 hours of the initiation of the surveillance.

S. 1566 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 fully the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence 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. The Senate committee is required to report annually to the Senate on the implementation of the bill.

II. STATEMENT OF NEED

The purpose of the Foreign Intelligence Surveillance Act is to provide legislative authorization and regulation for all electronic surveillance conducted within the United States for foreign intelligence purposes. It has long been recognized that foreign intelligence electronic surveillance, exempted from the warrant provisions of the Omnibus Crime Control Act of 1968, could be subject to abuse. The report of the Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities, issued in 1976, provided firm evidence that foreign intelligence electronic surveillances involved abuses and that checks upon the exercise of these clandestine methods were clearly necessary.

The basic premise of the bill is that a court order for foreign intelligence electronic surveillances can be devised that is consistent with the "reasonable search" requirements of the fourth amendment. The Supreme Court has not ruled on the question of Fourth Amendment standards for electronic surveillance of foreign powers and their agents within the United States, although the Court in the *Keith* case required a judicial warrant for domestic security surveillances not involving foreign powers.[3] Therefore, S. 1566 clarifies and advances the development of the law on a subject where uncertainty now exists.

The electronic surveillance authorized and regulated by this bill is designed to satisfy two broad types of intelligence requirements. First, it provides a means for the collection of "positive" foreign intelligence to enable the Government to understand and assess the capabilities, intentions, and activities of foreign powers. Second, it supplies a technique for use in foreign counterintelligence investigations to protect against clandestine intelligence activities, sabotage, and terrorism by or on behalf of foreign powers. The standards and procedures for electronic surveillance differ according to whether the primary purpose is collecting foreign intelligence or assisting foreign counterintelligence and counterterrorism investigations.

A. Foreign intelligence

The primary targets for electronic surveillance to collect foreign intelligence are "official" foreign powers: (1) foreign governments or their components; (2) factions of foreign nations, not substantially composed of U.S. persons; (3) entities which are openly acknowledged by foreign governments to be under their direction and control. Information acquired from the communications of these targets will typically relate to the national defense or security of the Nation, to the successful conduct of the foreign affairs of the United States, or to the ability of the United States to protect itself against actual or potential attack or other grave hostile acts of a foreign power or its agents.

For these types of surveillance the bill requires that a court determine *only* whether the target is an "official" foreign power. The court does not review the basis for the executive certification that the sur-

[3] *United States* v. *United States District Court*, 407 U.S. 297 (1972). But see *United States* v. *Butenko*, 494 F. 2d 593 (3d Cir. 1974). *United States* v. *Brown*, 484 F. 2d 418 (5th Cir. 1973); and *Tweibon* v. *Mitchell*, 516 F. 2d 594 (D.C. Cir. 1975).

veillance is needed to acquire foreign intelligence information, nor is it given a detailed description of the nature of the information sought or the means of surveillance to be used. The surveillance may last as long as a year before a new court order is required.

Even though the surveillance targets are not U.S. persons, substantial information about Americans may be acquired from surveillance of foreign powers. The primary role for the court in these circumstances is to ensure compliance with the requirement for minimization procedures governing incidentally acquired information concerning U.S. persons. Procedures are required to insure that, if the information relates solely to national security or foreign affairs interests, it is not disseminated in a manner that identifies a U.S. person unless the person's identity is needed to understand or assess information about a foreign power or unless the information is otherwise publicly available. The court may monitor compliance with these procedures.

Surveillance of certain foreign persons and certain foreign organizations, other than "official" foreign powers, may be conducted to obtain foreign intelligence. In such cases the judge is fully informed of (but does not review) the basis for the certification and is given a detailed description of the nature of the information sought and a statement of the means of surveillance to be used. Such surveillance may last only 90 days before a new court order is required. Foreign persons acting in the United States as officers or employees of foreign powers may be targeted for surveillance to collect foreign intelligence; but these requirements ensure that the information sought fulfills proper intelligence objectives and that the surveillance does not intrude unnecessarily into the personal privacy of the individual.

U.S. citizens, resident aliens, and foreign visitors to the United States may not be targeted for surveillance to collect foreign intelligence unless they also meet the separate foreign counterintelligence standards regarding terrorism, sabotage, or clandestine intelligence activities, discussed below. In the case of a U.S. person, the court would review the certification that the information sought is necessary for national security or foreign affairs purposes. Such judicial review of the Executive Branch certification, based on a "clearly erroneous" standard, occurs *only* if the surveillance target is a U.S. person.

In summary, the authority for surveillance to collect positive foreign intelligence varies according to the nature of the target and the type of information sought. Because the judicial role is very limited, it is the responsibility of the Attorney General and the certifying officials designated by the President to make determinations that take into account the characteristics of the foreign power, the risks involved, and the relevance of the information sought to the fulfillment of proper foreign intelligence objectives. Regular reporting to the Intelligence Committees of the House and Senate is also required to help insure that these surveillances are consistent with U.S. foreign policy, national defense needs, and appropriate standards of international conduct.

B. Foreign counterintelligence investigations

Electronic surveillance for foreign counterintelligence and counterterrorism purposes requires different standards and procedures. U.S.

persons may be authorized targets, and the surveillance is part of an investigative process often designed to protect against the commission of serious crimes such as espionage, sabotage, assassination, kidnaping, and terrorist acts committed by or on behalf of foreign powers. Intelligence and criminal law enforcement tend to merge in this area.[4] The targeting of U.S. persons and the overlap with criminal law enforcement require close attention to traditional fourth amendment principles.

S. 1566 departs from ordinary criminal law enforcement procedures in several ways. A judicial warrant is normally granted upon probable cause that a crime has been or is about to be committed. By contrast, in some cases the bill allows issuance of a court order upon probable cause that a person's activities "may involve" a criminal violation. Unlike the provisions of the Omnibus Crime Control Act of 1968 governing surveillance in regular criminal investigations, there is no listing of specific Federal criminal laws. Moreover, acts of sabotage and terrorism need not be violations of the criminal statutes of the United States, so long as they "would be criminal" under the laws of the United States or (in the case of terrorism) of any State if committed within this country. No showing of criminal activity is required where the target is a foreign person who acts on behalf of a foreign power which engages in clandestine intelligence activities contrary to the interests of the United States.

Additionally, surveillances conducted under S. 1566 need not stop once conclusive evidence of a crime is obtained, but instead may be extended longer where protective measures other than arrest and prosecution are more appropriate. The requirement of subsequent notice to the surveillance target is eliminated, unless the fruits are to be used against him in legal proceedings. *In camera* procedures are adopted for subsequent challenges to the legality of the surveillance.

The question is whether departures from traditional Fourth Amendment criminal procedures "are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens," as required by the Supreme Court's leading decision in this field, *United States* v. *United States District Court*, 407 U.S. 297, 323 (1972).

One approach to balancing these interests is the adoption of certain safeguards which are more stringent than conventional criminal procedures. S. 1566 does this in two ways. First, it requires the judge to review the certification that surveillance of a U.S. person is necessary for foreign counterintelligence purposes. Because the probable cause standards are more flexible under the bill, the judge must also determine that the executive branch certification of necessity is not "clearly erroneous."[5] Second, the bill provides for close and continuing com-

[4] Surveillance to collect positive foreign intelligence may result in the incidental acquisition of information about crimes; but that is not its objective. By contrast, foreign counterintelligence surveillance frequently seeks information needed to detect or anticipate the commission of crimes

[5] The "clearly erroneous" standard drawn from administrative law is more suitable here than the "probable cause" standard, which takes its meaning from the criminal law. The judge is required to review an administrative determination that, in the pursuit of a particular type of investigation, surveillance is justified to acquire necessary information. The judge may request additional information in order to understand fully how and why the surveillance is expected to contribute to the investigation.

munication with the congressional committees having jurisdiction over foreign intelligence activities. Such communication is inappropriate in conventional criminal cases where the objective is primarily prosecution and subsequent notice is served on the surveillance targets. But in the absence of notice or frequent judicial review in subsequent prosecution, as with criminal cases, congressional oversight supplies a compensating check.

Even with these added safeguards, the main issue is whether the investigative process in foreign counterintelligence cases requires specific departures from normal Fourth Amendment procedures. Based on its study of both electronic surveillance and foreign counterintelligence investigations, the Select Committee on Intelligence has concluded that such departures are reasonable. The need to preserve secrecy for sensitive counterintelligence sources and methods justifies elimination of the notice requirement, consolidation of judicial authority in a special court, and *in camera* procedures allowing persons to challenge illegal surveillance without endangering the security of legitimate surveillances.

The international character of foreign terrorist activities fully supports the more flexible probable cause standard allowing surveillance where foreign-based terrorist activities abroad "would" violate Federal or State laws if committed here. The United States has a duty to advise other nations if foreign agents within this country are mounting serious acts of violence to be committed outside our borders. We expect other countries to warn us when they learn of plans to commit serious violence in the United States; and this obligation should be reciprocal. The Federal Government also has an obligation to the States whose law enforcement agencies lack the capability of detecting foreign-based terrorist activities.

The absence of a list of specific Federal statutes furnishing the basis for surveillance, as in Title III, raises other considerations. With respect to terrorism, there is a limitation to violent acts on behalf of a foreign-based group which appear intended to intimidate or coerce the civilian population, to influence Government policy by intimidation or coercion, or to affect the conduct of government by assassination or kidnaping. There is no similar definition of the terms "clandestine intelligence-gathering activities" and "any other clandestine intelligence activities." The imprecision of these terms reflects an assessment of the nature and difficulty of foreign counterintelligence investigations.

The essential point is that, if electronic surveillance is to make an effective contribution to foreign counterintelligence, it must be available for use when necessary for the investigative process. The criminal laws are enacted to establish standards for arrest and conviction; and they supply guidance for investigations conducted to collect evidence for prosecution. Foreign counterintelligence investigations have different objectives. They succeed when the United States can insure that an intelligence network is not obtaining vital information, that a suspected agent's future access to such information is controlled effectively, and that security precautions are strengthened in areas of top priority for the foreign intelligance service. Prosecution is a useful deterrent, but only where the advantages outweigh the sacrifice of

other interests. Therefore, procedures appropriate in regular criminal investigations need modification to fit the counterintelligence context.

S. 1566 adopts probable cause standards that allow surveillance at an early stage in the investigative process by not requiring that a crime be imminent or that the elements of a specific offense exist. Surveillance of clandestine intelligence gathering activities that "may involve" a criminal violation, and of persons engaged in activities that "may be" in preparation for sabotage or terrorism, makes it possible to discover whether a person is likely to commit an offense in the foreseeable future.

On the other hand, because of the danger to activities protected by the first amendment, the standard for "clandestine intelligence activities" other than intelligence gathering requires probable cause that such activities are pursuant to the direction of a foreign intelligence service and that they "involve or are about to involve" a Federal crime. The bill also provides that no U.S. person may be considered an "agent of a foreign power" solely upon the basis of activities protected by the first amendment to the Constitution.

Finally, foreign counterintelligence surveillance of unofficial foreign visitors to the United States must meet the same probable cause standard as surveillance of U.S. persons, unless they act on behalf of particular foreign governments which engage in clandestine intelligence activities contrary to U.S. interests. Such surveillance is limited to persons who, on the basis of past experience with a particular foreign government, are reasonably believed to have clandestine intelligence assignments from the foreign government. It is intended to apply to visitors acting for foreign governments such as the Soviet Union which have used such visitors to the United States for clandestine intelligence purposes. This provision is tailored to demonstrated foreign counterintelligence requirements.

To summarize, the select committee's review of U.S. foreign counterintelligence requirements confirms the current relevance of the statement made 20 years ago in a study by the Fund for the Republic:

> The problems of crime detection in combating espionage are not ordinary ones. Espionage is a crime which succeeds only by secrecy. Moreover, spies work not for themselves or privately organized crime "syndicates," but as agents of national states. Their activities are therefore likely to be carefully planned, highly organized, and carried on by techniques skillfully designed to prevent detection.[6]

The response of the United States to such threats must be equally sophisticated, and S. 1566 provides techniques to satisfy this need.

C. Foreign intelligence surveillance and the fourth amendment

S. 1566 embodies a legislative judgment that court orders and other procedural safeguards are necessary to insure that electronic surveillance by the U.S. Government within this country conforms to the fundamental principles of the fourth amendment. The bill has been designed carefully to accommodate the two basic subdivisions of

[6] Fund for the Republic, *Digest of the Public Record of Communism in the United States*' (New York, 1955), p. 29.

United States intelligence requirements—collection of positive foreign intelligence and of information needed for foreign counterintelligence and counterterroism investigations.

In the first instance, surveillance solely to collect foreign intelligence is not targeted against U.S. citizens or resident aliens and distinctions are made among "official" foreign powers, other types of foreign organizations, and foreign persons who act as officers or employees of foreign powers. Because the purpose is unrelated to law enforcement and the targets are foreign powers or their officials, the fourth amendment may allow wider latitude in conducting reasonable research or surveillance operations designed to serve important national defense and foreign affairs interests. As former Attorney General Levi stated:

> "[A] central concern of the fourth amendment was with intrusions to obtain evidence to incriminate the victim of the search. This concern has been reflected in Supreme Court decisions which have traditionally treated intrusions to gather incriminatory evidence differently from intrusions for neutral or benign purposes. . . . Where the purpose or effect is noncriminal, the search and seizure is perceived as less troublesome and there is a readiness to find reasonableness even in the absence of a judicial warrant. By contrast, where the purpose of the intrusion is to gather incriminatory evidence, and hence hostile, or when the consequence of the intrusion is the sanction of the criminal law, greater protections may be given.[7]

Although foreign persons are protected by the fourth amendment when they are in the United States,[8] the noncriminal purpose, the limitation to officers or employees acting as such in the United States and the certification requirements satisfy the "reasonable search" standard of the Fourth Amendment as it may apply to surveillance conducted solely for the collection of foreign intelligence. Court orders simply ensure that the targets fit the categories and that minimization procedures limit the acquisition, retention, and dissemination of incidentally acquired information about U.S. persons. Congressional review supplies an added check.

Foreign counterintelligence surveillance may target U.S. persons and may involve detection of crimes, even though criminal prosecution may not result. The departures here from conventional Fourth Amendment doctrine have, therefore, been given close scrutiny to ensure that the procedures established in S. 1566 are reasonable in relation to legitimate foreign counterintelligence requirements and the protected rights of individuals. Their reasonableness depends, in part, upon an assessment of the difficulties of investigating activities planned, directed, and supported from abroad by foreign intelligence services and foreign-based terrorist groups. The differences between ordinary criminal investigations to gather evidence of specific crimes and foreign counterintelligence investigations to uncover and monitor clandestine activities have been taken into account. Other factors in-

[7] Church Committee Hearings, Vol. 5, pp. 75–76. See *Camara* v. *Municipal Court*, 387 U.S. 523 (1967); *Almeida-Sanchez* v. *United States*, 413 U.S. 266 (1973).
[8] *Abel* v. *United States*, 362 U.S. 217 (1960).

clude the international responsibilities of the United States, the duties of the Federal Government to the States in matters involving foreign terrorism, and the need to maintain the secrecy of lawful counterintelligence sources and methods.

An effort has been made to balance the need for surveillance at earlier stages of the investigative process and the protection afforded by the Fourth Amendment's requirement that searches for normal criminal law enforcement purposes be conducted only where a crime has been or is about to be committed. Because of the wider latitude granted by the bill, judicial review of the necessity for surveillance of U.S. persons and regular congressional oversight are required to ensure the proper exercise of administrative discretion.

That these departures from traditional Fourth Amendment criminal law enforcement standards are constitutional is supported by the Supreme Court's opinion in the *Keith* case. Although considering domestic security surveillance, the principles apply with even greater force to foreign counterintelligence surveillance. Justice Powell's opinion for the court states:

> [W]e do not hold that the same type of standards and procedures prescribed by title III are necessarily applicable to this case. We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.
>
> Given these potential distinctions between title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in title III. Different standards may be compatible with the fourth amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the government interest to be enforced and the nature of citizen rights deserving protection . . . It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of section 2518 [of title 18] but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court . . . ; and that the time and reporting requirements need not be so strict, as those in section 2518.

> The above paragraph does not, of course, attempt to guide the congressional judgment but rather to delineate the present scope of our own opinion. . . . We do hold, however, that prior judicial approval is required for the type of domestic security surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe. *United States* v. *United States District Court*, 407 U.S. 297, 322–324 (1972).

Far more than in domestic security matters, foreign counterintelligence investigations are "long range" and involve "the interrelation of various sources and types of information." Targets are often "difficult to identify," and the emphasis is primarily "on the prevention of unlawful activity." Where foreign governments and foreign-based organizations are the source of the danger, the Government clearly must prepare for a "possible future crisis or emergency." When clandestine intelligence and terrorist activities are planned, directed, and supported from abroad, rather than within the United States, the investigative task is extraordinarily difficult. Therefore, the focus of surveillance of suspected foreign agents must "be less precise" if the United States is to maintain adequate security.

The Select Committee on Intelligence believes the standards and procedures of S. 1566 reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights. S. 1566 would allow electronic surveillance in circumstances where, because of uncertainty about the legal requirements, the Government may otherwise be reluctant to use this technique for detecting dangerous foreign intelligence and terrorist activities by foreign powers in this country. At the same time it provides safeguards that have not existed before and that may reasonably be expected to prevent any recurrence of the abuses of the past.

Section-by-Section Analysis

Section 1 of the bill provides that the act may be cited as the "Foreign Intelligence Surveillance Act of 1978".

Section 2 of the bill amends title 18, United States Code by adding a new chapter 120 composed of sections 2521–2528 as follows:

Section 2521

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

A. "Foreign power"

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

(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 permanent resident aliens or citizens of the United States."

This category is intended to include factions of a foreign nation or nations which are in a contest for power over, or control of the territory of, a foreign nation or nations. The faction must be foreign-based and controlled from abroad. Specifically excluded from this category is any faction of a foreign government or governments which is substantially composed of permanent resident aliens or citizens of the United States. The word "substantially" means a significant proportion, but 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 court-ordered surveillance under a less stringent standard. That standard permits less information to be given to the judge and allows the surveillance to be continued for a longer period of time before reauthorization. Only entities "openly acknowledged" by a foreign government to be directed and controlled by it are subject to the extended court orders granted on a lesser showing.

Those entities which are clearly arms of a government or governments and not privately controlled meet this definition. This category would permit surveillance, for example, of a legitimate commercial establishment which is directed and controlled by a foreign government and which, because of the nature of its operations, constitutes a source of foreign intelligence information otherwise unavailable to the U.S. Government.

The committee is concerned about the possibility that many innocent U.S. persons might be employed by such entities, and that their offices and telephones could be subject to surveillance. The committee would have preferred that only entities not substantially composed of U.S. persons could be subject to surveillance as "foreign powers." If such, this requirement had been included in the bill, however, those entities could have hired a substantial number of Americans in order to avoid surveillance. To provide adequate protection for Americans, the Committee strengthened the "minimization" requirements to limit strictly the dissemination of information about U.S. persons where such information relates solely to national security or foreign affairs interests. See section 2521(b)(8), infra.

A law firm, public relations firm, or other legitimate concern that merely represents a foreign government or its interests is not 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 foreign-based terrorist group." This category refers to a foreign-based group engaged in "terrorism," as defined. The committee recognizes that international terrorist groups may have members from various nations and may not have any clearly definable "base." Under this definition the group must be "foreign-based"; that is, it may not be based in the United States. It is the committee's belief that a domestic terrorist group should not be subjected to electronic surveillance pursuant to this chapter. Where a group is not domestically based, but derives strength and refuge by organizing, planning, and

24-419 O - 78 - 3

preparing its terrorist activities or training its members outside the United States, then that group is a legitimate target for intelligence surveillance under this bill no matter what the citizenship of its members.

The committee does not intend to authorize electronic surveillance under any circumstances for the class of groups included by the Supreme Court within the scope of the *Keith* decision requiring judicial warrants for alleged threats to security of a purely domestic nature. The rare case might arise where a foreign-based terrorist group is substantially composed of U.S. persons. The judge must examine the circumstances carefully in order to determine whether the organization is a foreign-based terrorist group and not a domestic group with some foreign aspects to it. If there is significant doubt whether a terrorist group substantially composed of U.S. persons is foreign-based, the committee intends that this bill not apply. Instead, the Government may rely upon the domestic law enforcement surveillance procedures of title III of the Omnibus Crime Control Act of 1968, contained in chapter 119, United States Code.

(5) "A foreign-based political organization, not substantially composed of permanent resident aliens or citizens of the United States." This category is intended to include, for example, foreign political parties that are mere instrumentalities of a foreign government and that are not substantially composed of Americans. This category 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 arm of the government with respect to the 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 offer a means for evading the requirements for surveillance of individual 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 it itself sufficient to place the group in this category.

A revised definition of "United States person" insures that, where the entity is substantially composed of American citizens or permament resident aliens, minimization procedures will apply, and the judge will review, applying a "clearly erroneous" standard, the certification that surveillance of the entity is needed to acquire foreign intelligence information. See section 2521(b)(9), infra.

B. "Agent of a foreign power"

Subsection (b)(2) defines an "agent of a foreign power" in two separate ways. Subparagraph (A)(1) includes persons who are not U.S. persons and who act in the United States as officers or employees of a foreign power. The definition is framed in this way because it is presumed that nonresident aliens who act in the United States as officers or employees of a foreign power are likely sources of foreign intelligence or counterintelligence information. The definition excludes persons who serve as officers or employees 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. The subparagraph is otherwise not intended to encompass such foreign visitors as professors, lecturers, exchange students, performers, or athletes, even if they are receiving remuneration or expenses from their home government in such capacity.

Given the tenuous relationship of such officers and employees with the United States and their close relationship with a foreign power, this standard is considered to be reasonable in light of the Government's legitimate need for foreign intelligence and counterintelligence information and the nature of the interests upon which the search would intrude. There are several other limitations on such surveillance. An executive official must certify that the information sought from surveillance of an officer or employee of a foreign power relates to the national defense or security or to the successful conduct of foreign affairs, or that such information relates to the ability of the United States to protect against grave hostile acts, sabotage, terrorism, or clandestine intelligence activities. The committee does not intend that there should be indiscriminate surveillance of officers or employees of foreign powers within the United States. The judge will be informed of the type of information sought and the means by which the surveillance will be effected; and the surveillance may last no longer than 90 days before reauthorization. The judge will not, however, review the Executive Branch certification of need for the surveillance.

Subparagraphs (A)(ii) and (B) (i)–(iv) of subsection (b)(2) comprise the second definition of "agent of a foreign power." They define an agent in terms of the activities in which he is or may be engaged, or may engage, for or on behalf of a foreign power.

1. Foreign visitors

Subparagraph (A)(ii) 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 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 conspires with any person knowing that such person is engaged in such activities.

This category could potentially include any foreign visitor to the United States, but only if such visitor is acting for or on behalf of certain foreign powers. There is no specific requirement to show that the person may engage in activities which violate Federal criminal statutes.

This separate noncriminal standard for foreigners acting for or on behalf of certain foreign powers is a significant change from S. 3197, reported favorably by the committee during the 94th Congress, which treated foreign visitors the same as United States persons. It also differs from the foreign visitor standard proposed in S. 1566, as reported by the Judiciary Committee, which did not distinguish among the foreign powers for or on behalf of which a foreign visitor might act.

Concern has been expressed that, because the fourth amendment to the Constitution speaks in terms of protecting all "persons"—not just U.S. citizens and permanent resident aliens—the bill should not establish a different standard for foreign visitors. The committee has taken this concern into account in developing a standard that would satisfy compelling foreign counterintelligence requirements without subjecting foreign visitors to unequal treatment simply on the basis of their status as nonresident aliens.

Where there are compelling considerations of national security, alienage distinctions are lawful.[9] Those distinctions must, however, be carefully tailored to the demonstrated need and not be overly broad in their effects. That need has been established only with respect to foreign visitors who act for or on behalf of certain foreign powers. For example, the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church committee) pointed out that one quarter of the Soviet exchange students coming to the United States in a 10-year period were found by the FBI to be intelligence officers.[10] There is substantial information that each Soviet visitor to the West is approved by the Soviet security services, which control their passports and other aspects of their activities. It is reasonable to presume that certain Soviet visitors are either intelligence agents or "cooptees" who cooperate with Soviet intelligence. To the extent that other nations engage in similar practices, a comparable need arises.

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, it is not necessary to show that a visitor who falls into this class actually has an intelligence assignment.

As a practical matter in such circumstances, less intrusive investigative techniques may not enable the Government to obtain sufficient information about persons visiting the United States only for a limited time. Therefore, the additional showing required for U.S. persons may simply not be possible. What is required instead is a judicial finding of probable cause to believe that the person is acting for or on behalf of a foreign power which engages in clandestine intelligence activities contrary to the interests of the United States. The term "interests" refers to important and long-term goals of the United States, including inter-

[9] See, e.g., *Hampton* v. *Mow Sun Wong*, 426 U.S. 88, 116 (1976).
[10] *Final Report*, book I, p. 164.

ests embodied in law. The Committee does not intend to include foreign governments whose clandestine intelligence activities are merely contrary to U.S. policy, rather than contrary to the law or other national interests. Once the requisite facts with regard to the country are established, the question is whether the circumstances of the person's presence in the United States indicate that the person may engage in such activities. The answer to this question will vary according to what we know about the intelilgence operations of the particular foreign power. Among the factors that might be taken into account are whether the foreign visitor is in the United States under the auspices of the foreign power and whether he engages in activities with respect to which there is evidence that other visitors who engage in similar activities are officers or agents of the intelligence service of that foreign power or a cooperating foreign power.

The standard "may engage in such activities" means that surveillance can be conducted to anticipate clandestine intelligence 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 harmful clandestine intelligence activities. The "knowingly" requirements are the same as in the aiding or abetting and conspiracy standard for U.S. persons. See section 2521 (b) (2) (B) (iv), 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.

2. Clandestine intelligence gathering

Subparagraph (B) (i) allows surveillance of any person, including a U.S. 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. Under this standard the person to be under surveilance must be shown to have a knowing and substantial connection with the foreign power for which he is working. There must be a relationship under which the alleged agent has undertaken to provide services for the foreign power. The Committee wishes to stress that this bill is not intended to authorize electronic surveillance under any circumstances for the class of individuals who pose alleged threats to security of a purely domestic nature for which the Supreme Court required a warrant in the *Keith* case.

The agent must also be knowingly engaged in "clandestine intelligence gathering activities" that involve or may involve violations of Federal criminal law. It is anticipated that most of the persons under surveillance under this subparagraph will be violating the criminal espionage laws which appear in title 18, United States Code, sections 792–799, 951; title 42, United States Code, sections 2272–2278b; and title 50, United States Code, section 855. The term "clandestine intelligence gathering activities" includes collection or transmission of in-

formation or material that is not generally available to the public, or covert contacts with an intelligence service or network by means of "drops" or other methods characteristic of foreign intelligence operations. In addition to activities that fall within the substantive statutory definition of spying are activities directly related to spying that may constitute violations of laws proscribing the aiding and abetting of spying, such as maintaining a "safehouse" for secret meetings, servicing "letter drops" to facilitate covert transmission of instructions or information, recruiting new agents, or infiltrating and exfiltrating agents under deep cover to and from the United States.

Apart from the types of activities specifically proscribed by the espionage laws, this subparagraph is also intended to permit the surveillance of foreign intelligence agents who are collecting industrial or technological information which, if disclosed to a hostile foreign power, might present a threat to the security of the Nation. In such a case, the Government would have to establish that the agent was collecting or transmitting such information in a manner which might involve a violation of some other Federal statute, such as title 18, United States Code, section 2514, which proscribes the interstate transportation of stolen property. In some cases the knowing transfer of technological information to a foreign country without a license from the Federal Government might be unlawful under the "Export Administration Act," title 50, United States Code, sections 2021–2032 or the International Traffic in Arms Regulations (22 CFR 121 et seq.).

Otherwise, clandestine collection of information regarding the unclassified business plans or trade secrets of an American company which merely might provide a competitive advantage to private foreign firms, for example, in bidding on a contract with a third country, would not be "clandestine intelligence gathering activity."

Moreover, the gathering of information which is done in a confidential manner as part of lawful political activity—such as gathering "intelligence" about the political strength and plans of proponents or opponents of a particular policy—would not constitute "clandestine intelligence gathering activity" under this subparagraph, where such information gathering is a normal ancillary part of lobbying, organizing political protest, and other political activity protected by the first amendment.

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.

Whatever the nature of the information or material gathered or transmitted by the foreign agent, there must be a clandestine aspect. The bill requires that the alleged foreign agent not only be working for or on behalf of a foreign power, but also, as a separate requirement, that he be engaged in clandestine intelligence gathering activity.

There must also be an effort to obtain information which is being kept secret or is not otherwise generally available to the public, or not available to the general public. Therefore, the collection, for whatever purpose, of information within the public domain such as that con-

tained in books, magazines, scientific journals, or newspapers would not constitute "clandestine intelligence gathering activity" under this subparagraph.

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 previous noncriminal standard which appeared in S. 3157, as reported favorably by the committee during the 94th Congress, and in S. 1566 as reported by the Judiciary Committee. 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 hostile 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 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 circumstances into account—who the person is, where he is employed, whether he has access to classified or other sensitive information, the nature of the clandestine meetings, the method of transmission, and whether there are any other reasonable 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 surveillance at some point prior to the time when a crime sought to be prevented, for example transfer of classified documents, actually occurs. There does not have to 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." Under the extension provisions of section

2525(c), discussed infra, the judge can insist on examining the fruits of any earlier surveillance when it is necessary to determine whether there is probable cause to believe that the individual is engaged in clandestine intelligence gathering activities that "may involve" a Federal criminal violation. Surveillance cannot be justified unless there is probable cause to believe that the person is, currently, engaged in such activities, even though the relationship of those activities to a specific law violation may be more uncertain or remote in time.

Finally, it is necessary that the person be aware he is acting for or on behalf of a foreign power. A person might be secretly collecting information about important technology, for example, and have been misled into the belief that he was acting for a research institute or a multinational corporation. Surveillance of such person would not meet the standard of this subparagraph. It also follows, of course, that evidence of efforts of a foreign power to recruit a person as an agent would not suffice to establish probable cause to believe the person has agreed to do the foreign power's bidding and is engaged on its behalf. Before electronic surveillance could be directed against such person, the court would have to find probable cause that he has been acting for that power's intelligence network.

3. Other clandestine intelligence activities

Subparagraph (B)(ii) allows surveillance of any person, including a U.S. 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. Under this standard the person must not only have a knowing and substantial connection with the foreign power, but he also must be acting pursuant to the direction of a foreign intelligence service or network.

The words "involve or are about to involve" are intended to require that a Federal crime must have already been committed, or must be about to occur, before surveillance is justified under this subparagraph.

These more stringent requirements are necessary because of the nebulous character of the term "any other clandestine intelligence activities," which can border upon the exercise of rights protected by the first amendment. Such intelligence activities may include covert actions designed by an intelligence service of a foreign power to influence events in this country. However, only if such covert political action involves a present or imminent violation of federal criminal law, such as title 18, United States Code, section 201 (bribery of public officials) and is undertaken pursuant to the direction of an intelligence service of a foreign power, would it be encompassed by this subparagraph. It does not authorize electronic surveillance under any circumstances for the class of individuals who pose alleged threats to security of a domestic nature for which the Supreme Court required a judicial warrant in the *Keith* case.

It is the intent of this requirement that even if there is some substantial contact between domestic groups or individual citizens and a

foreign power, as defined in this bill, no electronic surveillance under this subparagraph may be authorized unless the American is acting under the direction of an intelligence service of a foreign power. Excluded, for example, are Americans of Greek, Jewish, Irish, or Chinese extraction who legitimately seek to influence U.S. policy toward the country of their ethnic origin. In the process, such Americans are likely to be in communication with representatives of the governments of those countries in order to learn about particular situations or problems. If an American formulates lobbying efforts in part on the basis of such advice or suggestions he could, in one sense, be said to be following the direction of a foreign power. But this subparagraph requires that the agent act pursuant to the "direction of an intelligence service or network of a foreign power." Thus, such direction from persons who are not connected with an intelligence service or network would not be a basis for electronic surveillance under this subparagraph. There would have to be information specifically indicating the Americans had undertaken to do the bidding of an intelligence service or network, or its agents, rather than merely acting because of an affinity for the same concerns as that foreign power. Mutual goals or common concerns are not sufficient.

Another example of Americans having contact with foreign powers is the case of Americans who were active in the protest against U.S. involvement in Vietnam. Some of them may have attended international conferences at which there were representatives of foreign powers, as defined in the bill, or may have been directly in communication with foreign governments concerning this issue. There may have been an exchange of information about activities protesting the Vietnam war. But if there merely was evidence that an American was coordinating the dates of planned peace demonstrations in the United States to coincide with similar activities abroad in order to maximum worldwide public attention, that would not suffice to find probable cause that the American was acting under the direction of a foreign intelligence service as required by this subparagraph. Additional evidence would have been required indicating that the American had undertaken to follow the instruction of a foreign intelligence service or network, rather than simply trying to coordinate his independent effort with related activities abroad.

For both of these illustrations, it should be emphasized that even if there was probable cause to believe an American was acting pursuant to the direction of a foreign intelligence service, the court would also have to find probable cause to believe that the American had committed or was about to commit a Federal crime. This is a separate and distinct requirement.

Further, an organization substantially composed of Americans, whether residing in the United States or abroad, would not come within the definition of acting pursuant to the direction of a foreign intelligence service merely because it was part of a worldwide confederation of national organizations. Even if a domestic organization were found to be acting through its leaders at the direction of a foreign intelligence service, an individual's mere membership in that organization, without more information about his own undertaking to do so, would not constitute probable cause to believe that that par-

24-419 O - 78 - 4

ticular member was acting pursuant to the direction of a foreign intelligence service for purposes of this subparagraph.

It is necessary that the person be *aware* he is acting on behalf of a foreign power. It would not suffice to establish probable cause that the American is engaged in a covert activity at the direction of a foreign power; the government must establish probable cause that the American knows his efforts are on behalf of a foreign power.

4. Sabotage or terrorism

Subparagraph (B) (iii) allows surveillance of any person, including a U.S. person, who knowingly engages in sabotage or terrorism, or activities which are or may be in preparation therefor, for or on behalf of a foreign power. This standard differs from S. 3197, as reported favorably by the committee in the 94th Congress, which covered any person who "knowingly engages in or knowingly acts in furtherance of," sabotage or terrorism for or on behalf of a foreign power. It also differs from S. 1566, as reported by the Judiciary Committee, which adopted the standard "knowingly engages in activities that involve or will involve sabotage or terrorism for or on behalf of a foreign power." The committee has modified these earlier standards in order to accommodate the need to anticipate serious terrorist crimes. The words "will involve" in the bill as reported by the Judiciary Committee require too high a degree of certainty that terrorism will take place, especially compared to the "may involve" standard for spying in subparagraph (B) (i).

The terms "sabotage" and "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 or may be in preparation" for sabotage or terrorism is intended to encompass activities supportive of acts of serious violence—for example, purchase or surreptitious importation into the United States of explosives, planning for assassinations, or financing of or training for such activities.

The term "preparation" does not require evidence of preparation for one specific terrorist act, because the definition of "terrorism" speaks of "violent acts" and means a range of acts, not just a single act. "Preparation" normally means preparation for a specific crime, which might be too strict a standard for surveillance under this bill. However, the term "preparation" would not have its normal meaning because of the special definition of "terrorism." It 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 "preparation" provision is also adopted 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.

Concern has been expressed that this subparagraph could permit surveillance solely on the basis of information that someone might com-

mit acts of terrorism or sabotage in the distant future. This is clearly not the intent of the committee. There must be a showing of activities which may be in preparation for the commission of such acts. The committee has concluded, however, that surveillance is justified on the basis of somewhat less information regarding the nature of this activity than would be required in the absence of the words "may be." Under the extension provisions of section 2525(c), discussed infra, the judge can insist on examining the fruits of any earlier surveillance when it is necessary to determine whether there is still probable cause to believe that the individual may be preparing for sabotage or terrorism.

This subparagraph would allow surveillance where the Government cannot establish probable cause that an individual has knowingly engaged in preparation for sabotage or terrorism, but where there are sufficient specific and articulable facts to indicate that the individual's activities may be in preparation for sabotage or terrorism. As with the "may involve" standard of subparagraph (B)(i), 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 may be in preparation for sabotage or terrorism.

Finally, any person targeted for surveillance under this subparagraph must be shown to have a knowing and substantial connection with the foreign power for whom he is working. In the case of terrorism, it is anticipated that in most cases this connection will be shown to exist with a foreign-based terrorist group. The person must be clearly and knowingly acting for or on behalf of the foreign power itself. As elsewhere in this bill, the committee does not intend to authorize electronic surveillance under any circumstances in which a warrant would be required by the Supreme Court decision in the *Keith* case.

The rare case might arise where a U.S. person is acting for or on behalf of a foreign-based terrorist 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 foreign-based terrorist group and not a domestic group with some foreign aspects to it. Where there is significant doubt as to whether a terrorist group substantially composed of U.S. persons is foreign-based, the committee intends that the provisions of this bill should not apply to a person acting for or on behalf of such group. Instead, the Government may 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.

5. Aiding or abetting and conspiracy

Subparagraph (B)(iv) 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 (B) (i)–(iii) above, or conspires with any person knowing that such person is engaged in such activities. The knowledge requirement is applicable to both the status of the person being aided by the proposed subject of the sur-

veillance 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 terrorist activities 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 knowlingly aids or abets a foreign agent.

6. First amendment proviso

Subparagraph (B)(iv) concludes with a proviso which applies to all the foregoing standards for surveillance of U.S. persons. It provides that no U.S. person may be considered 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, stated earlier, that lawful political activities should never be the sole basis for a finding of probable cause to believe that a U.S. person is an agent of a foreign power. For example, the advocacy of violence falling short of incitement 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 estabilsh probable cause that an individual may be preparing for the commission of such acts.

The committee does not intend that information concerning pure advocacy of violence should be completely excluded from consideration by the judge in making such a probable cause finding, if facts regarding other activities not protected by the first amendment, such as the purchase of a weapon, are present. Activities not protected by the first amendment, however, must be the primary basis for the probable cause finding.

The bill is not intended to authorize electronic surveillance when a United States person's activities, even though secret and conducted for a foreign power, consist entirely of lawful acts such as lobbying or the use of confidential contacts to influence public officials, directly or indirectly, through the dissemination of information. Individuals exercising their right to lobby public officials or to engage in political dissent from official policy may well be in contact with representatives of foreign governments and groups when the issues concern foreign affairs or international economic matters.

They must continue to be free to communicate about such issues and to obtain information or exchange views with representatives of foreign governments or with foreign groups, free from any fear that such contact might be the basis for probable cause to believe they are acting at the direction of a foreign power thus triggering the Government's power to conduct electronic surveillance. The intent of the bill is to exclude from the definition of "clandestine intelligence activities" any activity which consists solely of the lawful exercise of first amendment rights of speech, petition, assembly, and association. In no event may lawful political activity within the ambit of the protections afforded by the first amendment be the basis for finding that any United States person is engaged in "clandestine intelligence activities." Lobbying Congress or seeking to influence public opinion on matters relating to the national defense or foreign affairs does not become clandestine intelligence activity merely because the agent has failed to comply fully with the Foreign Agents Registration Act (22 U.S.C. 611, et. seq.). If, however, foreign intelligence services hide behind the cover of some person or organization in order to influence American political events and deceive Americans into believing that the opinions or influence are of domestic origin and initiative and such deception is willfully maintained in violation of the Foreign Agents Registration Act, then electronic surveillance might be justified under subsection (B)(ii) if all the other criteria of S. 1566 were met.

The committee does not intend that the conspiracy provision of subsection (B)(iv) should be interpreted to permit surveillance based solely upon the combination of ambiguous public statements expressing a general intent to violate the law and an unambiguous public statement of such intent, in the absence of facts regarding any other specific acts taken to carry out such intent.[11]

Mere membership in a political group directed and controlled by a foreign power is not sufficient under this bill to establish probable cause that a person is aiding or abetting or conspiring with someone for or on behalf of a foreign power or engaged in clandestine intelligence activities. Moreover, even if additional information established

[11] C.F., *Spock, et al. v. United States*, 416 F. 2d 165 (1st Cir. 1969).

probable cause to believe some members of the group were aiding or abetting or conspiring with persons acting for or on behalf of a foreign power, neither efforts to collect information about the plans and program of the civil rights movement or other political protests, nor efforts to stimulate or shape them would constitute clandestine intelligence activity within this section. Gathering information about the movement would be neither criminal espionage nor the kind of economic or technical information relating to the national security whose collection might involve the violation of any other Federal law. Similarly, since the civil rights movement itself involved constitutionally protected rights of association, speech and petition for redress of grievances, efforts by a foreign power to involve itself in such a movement are intended to be specifically excluded from the clandestine intelligence activity standard for targeting U.S. persons.

C. "Terrorism" and "sabotage"

Subsection (b)(3) defines "terrorism" as acts which are violent or dangerous to human life and which would be criminal under the laws of the United States or of any State if committed within its jurisdiction. The words "would be" are used here, and in the definition of "sabotage," to indicate that the acts need not, in fact, be violations of Federal or State law, so long as they would constitute such violations if committed within the jurisdiction of the United States or of any State. 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 is 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 government to prevent its territory from being used as a base for launching terrorist attacks against other countries. 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 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 such activities 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.

Subsection (b)(4) defines sabotage as activities which would constitute crimes under chapter 105 of title 18, United States Code, if conducted against the United States. In S. 3197 only actual violations of chapter 105 were included in the definition of sabotage. But by its terms, chapter 105 makes criminal only acts of sabotage against U.S. Government facilities. S. 1566 has expanded 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.[12] 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 and the information sought constitued foreign intelligence as defined. Where persons are 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.

D. Foreign intelligence information

Subsection (b)(5) defines foreign intelligence information according to whether or not the information concerns a U.S. person. The comparable provision in S. 1566, as reported by the Judiciary Committee, is modified in order to apply the more stringent requirements solely to information about U.S. persons.

The committee has dropped the distinction between "necessary" and "essential" in the standard. The difference between the two terms is marginal, and using a single term has advantages of clarity and consistency. The committee has also deleted the word "deemed"; instead, an Executive Branch official will be required to certify that the information sought from each surveillance is deemed to be foreign intelligence information. See section 2524(a)(7)(A), infra.

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 prove an important piece of the larger picture. In that sense, any information relating to the specified purposes might be called "necessary" but such a reading is clearly not intended.

Information concerning U.S. persons is foreign intelligence information if it is necessary to the national defense or security, to the successful conduct of foreign affairs, or to the ability of the United States to protect against grave hostile acts, sabotage, terrorism, or clandestine intelligence activities by or on behalf of foreign powers. Information concerning foreign powers and foreign persons is foreign intelligence information if it relates to those interests.

Subparagraph (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 itself 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,

[12] Under 18 U.S.C. 956, it is a Federal crime for persons within the United States to conspire to injure or destroy property located in a foreign country and owned by a foreign government.

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 on the United States. Thus, only grave types of hostile acts would be envisioned as falling within this provision.[13]

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

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

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. The term "national defense or the security of the Nation" is intended to mean military and defense concerns. It is not a catchall term "national security" to be used to mean anything the Executive Branch wants it to mean. With these limitations, the committee believes that the adoption of a "relates to" standard would not authorize improper treatment of foreign persons who come to the United States. In this regard, of course, the committee's oversight authority is another valuable check.

---

[13] In testifying in 1976 at the House hearings on S. 3197, Attorney General Levi confirmed this interpretation:

"Mr. KASTENMEIER. How do you understand the term other hostile acts of a foreign power? Is there enough precedent or other language so that we understand precisely what the hostile acts constitute, whether a criticism of our participation in the Vietnam war would be a hostile act? Or attempting to board an American ship on the high seas is a more classical case. How broad is the hostile acts?

"Attorney General LEVI. I certainly wouldn't think that hostile acts involved criticism. I would assume—I don't know that we can get a better definition. But it does after all say, 'against actual or potential attack or other hostile acts.' So that it is the actual or potential attack which really gives the flavor to what is meant.

"Mr. KASTENMEIER. In other words, it must be seen in a broader context, and therefore be much more limited?

"Attorney General LEVI. I would think so." (1976 House hearings 10–11.)

Subparagraph (C) (i) 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 2521(b)(1)(D), or against the type of foreign agent defined in section 2521(b)(2)(B)(iii).

Subparagraph (C)(ii) 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 of an intelligence service or network of a foreign power or a foreign agent. This subparagraph encompasses classic counterintelligence information; that is, information deemed necessary to the Nation's ability to discover and protect against the clandestine intelligence activities of foreign powers or their agents in the United States. 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 "news leaks" 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 and that such publication would 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 relates to his activities on behalf of a foreign power. This is achieved by including in each subsection of the foreign intelligence definition the requirement that the information sought actually "relates to" the type of information that is necessary. For example, the Government could not seek purely personal information about a U.S. citizen or permanent resident alien, who is a suspected spy, upon a theory that it might learn something that would be "compromising." The bill makes clear that only information about U.S. citizens or permanent resident aliens that is necessary to the ability of the United States to protect against clandestine intelligence activities may be sought. This restriction might now always be fully applicable to agents of foreign powers as defined in section 2521(b)(2)(A)(i) or (ii), because information about their private lives may itself be foreign intelligence information. For example, such information might identify their true status or reveal the intentions or activities of the foreign power of which they are officers or employees.

E. Electronic surveillance

Subsection (b)(6) defines electronic surveillance to include four separate types of activities.

Subparagraph (A) 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. Under S. 3197 as reported by the committee in the 94th Congress, such targeting did not fall within the confines of the bill; this provision is, therefore, a significant extension of the protections afforded U.S. citizens and resident aliens. The subparagraph 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. citizen or resident alien, provided that the person is located within the United States. Thus, for example, the watchlisting activities of the National Security Agency, if directed against the international communications of particular U.S. persons who are in the United States, would require a court order under this provision.[14]

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 subparagraph (A). 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 definition of "wire communication" under 18 U.S.C. 2510(1) covers any communication "made in whole or part" through wire facilities. Excluded would be, for example, commercial broadcasts, as well as ham radio and citizen band radio broadcasts [cf. 47 U.S.C. 605; *United States* v. *Hall*, 488 F. 2d 193 (9th Cir. 1973)].

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.[15] 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 subparagraph does not apply to the acquisition of the contents of international or foreign communications, where the contents are not 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 is concerned about the need to provide statutory protections and regulations in this area, but does not believe that

[14] 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, for careful documentation of the nature of such National Security Agency activities undertaken on behalf of the FBI, CIA, Army intelligence, and the Bureau of Narcotics and Dangerous Drugs, and the technological problems associated with authorized NSA signals intelligence activities.

[15] 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 wire tapped for different purposes. Such a case has occurred in the past. See *Church Committee Report, book II*, p. 228.

S. 1566 is the appropriate vehicle for doing so. The standards and procedures for overseas surveillance may have to be different than those provided in S. 1566 for electronic surveillance within the United States or targeted against U.S. persons who are in the United States. Instead, members of the committee have introduced as part of S. 2525, the National Intelligence Reorganization and Reform Act of 1978, separate legislation to achieve this objective.

The fact that S. 1566 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.[16]

Subparagraph (B) 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 while the communication is being transmitted by wire. 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 and if such acquisition occurs "while the communication is being transmitted by wire." This second qualifier is necessary because the definition of "wire communication" under 18 U.S.C. 2510(1) includes any communication "made in whole or in part" through wire facilities. Because most telephonic and telegraphic communications are transmitted at least in part by microwave radio transmissions, subdefinition (B) is meant to apply only to those surveillance practices which are effected by tapping into the wire over which the communication is being transmitted. The interception of the microwave radio transmission is meant to be covered by subdefinition (C) if the sender and all intended recipients are located within the United States, or by subdefinition (A) if it is done through the targeting of a U.S. person who is in the United States.

The surveillance covered by subparagraph (B) 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

---

[16] 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. Thus, the surveillance of journalists, such as in the *Joseph Kraft* case, would be prohibited.

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 S. 1566 is the appropriate measure in which to do so. As introduced, S. 2525, the National Intelligence Reorganization and Reform Act of 1978, provides certain statutory safeguards in this area.

Subparagraph (C) 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 definition would reach not only the acquisition of communications made wholly by radio but also the acquisition of "wire communications" by means of intercepting the radio transmitted portion of those communications within the United States. The territorial limits of this subdefinition are not dependent on the point of acquisition, as is the case with subdefinition (B), but on the locations of the sender and intended recipients. 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 wire communication being transmitted by 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 contents, as described with respect to subparagraph (B).

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, S. 1566 would require the destruction of such contents in almost all circumstances. See Sec. 2526(g), infra.

The effect of this amendment, in combination with subparagraphs (A), (B), and (C) of this subsection, is to apply either a destruction requirement or a court order requirement for the nonconsensual acquisition of all domestic radio communications made with a reasonable expectation of privacy, the nonconsensual acquisition within the United States of all wire communications, as defined in section 2510 (1), title 18, United States Code, and the targeting of particular

United States persons located in the United States in order to acquire domestic or international communications made with a reasonable expectation of privacy.

Subparagraph (D) brings within the definition of "electronic surveillance" the acquisition of information, not transmitted as a wire communication or radio communication, by the installation or use of an electronic, mechanical, or other surveillance device 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 judicial review. It is not meant to include, however, the acquisition of those international radio transmissions or international wire communications, when acquired by intercepting radio transmissions, which are 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.[17] But two persons in a public park, far from any stranger, would not reasonably anticipate that their conversations could be overheard from afar through a directional microphone, and so would retain their right of privacy.

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 perpetuate the 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.[18] Whether consent may be inferred in a particular case will depend on the facts and circumstances. The other parts of the definition 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 informer may

[17] *Air Pollution Variance Board* v. *Western Alfalfa Corp.*, 416 U.S. 861 (1974).
[18] *Lopez* v. *United States*, 373 U.S. 427 (1963); *Rathbun* v. *United States*, 355 U.S. 197 (1957).

have no justifiable expectation that the informer will not repeat, record, or even transmit by a miniature transmitter what the person voluntarily tells the informer.[19]

The committee does not intend the term "surveillance device" as used in subparagraph (D) 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 is desirable to develop legislative controls over physical search techniques, the committee has concluded that these practices are sufficiently different from electronic surveillance as to require separate consideration by the Congress. S. 2525, the National Intelligence Reorganization and Reform Act of 1978, addresses the problem of physical searches within the United States or directed against U.S. persons abroad for intelligence purposes. The fact that S. 1566 does not cover physical searches for intelligence purposes should not be viewed as congressional authorization for such activities. In any case, the requirements of the fourth amendment would, of course, continue to apply to this type of activity.[20]

Except for the use of a surveillance device as an incident to physical search or mail opening, the term "device for monitoring" would apply in any circumstances where a warrant would be required for law enforcement purposes.

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 subparagraph (A), (C), or (D). The techniques involved may not have been used for law enforcement purposes, or if so used, may not have come before a court for a determination as to whether a warrant is required. Nevertheless, the surveillance activity is intended 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 has with respect to such activity. The committee expects that, if an agency wishes to use a related 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 under the provisions of section 2528.

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.

F. "Attorney general"

Paragraph (7) defines "Attorney General" to mean the Attorney General of the United States, the Acting Attorney General, or the

---

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

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

Deputy Attorney General. Under S. 3197 as reported in the 94th Congress, only the Attorney General or the Acting Attorney General could approve an application for an electronic surveillance order. S. 1566 as originally 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.

With the assurance of Attorney General Bell in his testimony before the Judiciary Committee on S. 1566 that he would personally continue to approve applications under the bill until standards of review have been well established, that committee 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. This committee endorses that approach. 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.

G. "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 (8) defines "minimization procedures" as procedures reasonably designed to minimize the acquisition and retention, and prohibit the dissemination, except as provided in subsections 2526 (a) and (b), of any information concerning U.S. persons not related to certain purposes. Specifically, information concerning Americans must be related to the ability of the United States to protect itself against actual or potential attack or other grave hostile acts of a foreign power or agent of a foreign power, to provide for the national defense or security of the Nation, to provide for the conduct of the foreign affairs of the United States, to protect against terrorism or sabotage by foreign powers or their agents, or to protect against the clandestine intelligence activities of a foreign intelligence service or an agent of a foreign power.

The minimization requirement of this paragraph is meant generally to parallel the minimization provision in existing law. (18 U.S.C. 2518 (5)). As the courts have noted in construing that section, "It is . . . obvious that no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." [21] In assessing the minimization effort, the court's role is to determine whether "on the

[21] *United States* v. *Bynum*, 485 F. 2d 490, 500 (2nd Cir. 1973), cert. denied 423 U.S. 1005 (1975).

whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could to avoid unnecessary intrusion." [22] Absent a charge that the minimization procedures have been disregarded completely, the test of compliance is "whether a good faith effort to minimize was attempted." [23]

Among the factors to be considered in evaluating the reasonableness of the agents' conduct will be the scope of the enterprise under investigation, the location and operation of the subject telephone (or microphone), the Government's expectations of the character of and parties to the calls, and the length or brevity of the monitored conversations.[24] Minimization procedures may differ depending on the nature of the relationship to a foreign power, the individuals using the facilities or place to be surveilled, the type of foreign intelligence information sought, and other similar factors. Minimization procedures might also include restrictions on the use of surveillance to times when foreign intelligence information is likely to be obtained, directions that the surveillance cease if it does not produce results of the specified type, requirements that conversations not involving the named target be deleted from the records at an appropriate time, and other requirements. For example, if a citizen or permanent resident alien were using facilities of a foreign agent that were the target of the surveillance, the Government would be required to minimize the acquisition and retention of any information that did not relate to foreign intelligence purposes.

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, would be discontinued as soon as it was realized that she rather than A was the party. In other cases, however, primarily for technological reasons, it may not be possible to avoid acquiring all conversations. In these situations minimizing retention and dissemination becomes most important. By minimizing retention, the committee intends that information acquired, which does not relate to the approved purposes in the minimization procedures, be destroyed. 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, would be destroyed. Indeed, even A's communications which are clearly not relevant to his clandestine intelligence activities should be destroyed. In certain cases destruction would 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 to be approved by the court and are, of course, subject to judicial supervision.

---

[22] *United States* v. *Tortorello*, 480 F. 2d 764 (2nd Cir.), cert. denied 414 U.S. 886 (1973).
[23] *United States* v. *Armocida*, 515 F. 2d 29, 44 (3d Cir. 1975).
[24] *United States* v. *Armocida*, *supra*; *United States* v. *James*, 494 F. 2d 1007 (D.C. Cir. 1974), cert. denied 419 U.S. 1020 (1975); *United States* v. *Bynum*, *supra*.

A Judiciary Committee amendment to the minimization definition makes explicit the intent that information not related to an approved purpose not be disseminated. The only exceptions to this prohibition recognized by the bill are for one of the purposes authorized in section 2521(b)(8), or for the enforcement of the criminal law under the provisions of section 2526 (a) and (b). Under the dissemination phrase, information being held to determine relevancy would not be disseminated until the determination was made (or would only be disseminated to those who could determine its relevancy). It should also mean that, even with respect to information relevant to an approved purpose, dissemination would 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.

In short, the committee believes that the definition of minimization procedures authorizes and requires that information concerning American citizens and resident aliens be handled in such a way as to assure that it is used only for the purposes specified in the definition and not for any other purpose. Some have suggested that the statutory definition is too general. The committee recognizes, however, that minimization requirements which are appropriate for some types of surveillances would be inappropriate for others. A certain flexibility in the statute is, therefore, necessary with careful judicial scrutiny of a particular application constituting the best protection against abuse. But the definition does not give carte blanche to the judge. It requires that the procedures be designed to limit the acquisition, retention, and dissemination of information concerning American citizens and lawful resident aliens to that information which is related to one of the approved purposes; in addition, the procedures must provide that the information obtained by the surveillance will not be used for an unrelated purpose (other than for enforcement of the criminal law, see section 2526(a), infra).

Of course, minimization applies only to information known to concern U.S. persons. Where communications are encoded or otherwise not processed so the contents of a communication are not known, it would not be possible to minimize the acquisition, retention, and dissemination of information concerning U.S. persons. Nevertheless, the minimization procedures can be structured to apply to other agencies of the Government, so that if an agency different from the intercepting agency decodes or processes the communication, it could be required to minimize the retention and prohibit the dissemination of information therein concerning U.S. persons.

It should be noted that this provision contains one significant change from the minimization provisions in chapter 119. 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

24-419 O - 78 - 6

purpose 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 procedures approved by the court. 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, interceptions which are destroyed.

The committee is concerned that the surveillance authorized under this chapter not result in the retention or dissemination of information which would adversely affect the exercise of first amendment rights. Such abuses occurred with distressing frequency in the past. Information relating solely to the lawful political activity of American citizens or resident aliens may not be retained or disseminated under the provisions of this legislation.

In a hypothetical case, for example, an ambassador from an important neutral nation, speaking to a U.S. Senator, tells the Senator that his country has been approached secretly by a foreign nation concerning a planned attack on the United States. Assuming that the surveillance was initiated against the ambassador and approved in accordance with the procedures of this chapter, there should be no doubt that the information could be retained and used because of its importance and relationship "to the ability of the United States to protect itself against actual or potential attack." At the same time, however, the constitutional rights of speech, association, and privacy of the Senator are implicated. He is plainly not the target of the surveillance, nor could he be, since he is not the "agent of a foreign power." Still he is overheard. The functioning of democratic government can be impaired if its representatives are deterred from discussing important issues with representatives of other countries for fear that their conversations will be overheard and retained.

There is no perfect solution to the problem. As long as the surveillance was instituted lawfully, the Senator's conversation may be overheard. Given the subject matter of the conversation, it should not be excluded by minimization procedures. If the subject matter relates to foreign intelligence purposes, the information should be retained. The alternative—a blanket rule depriving the Government of the right to retain foreign intelligence, regardless of its importance, because an American citizen was incidentally overheard—is unacceptable. Similarly, it would not be advisable to obligate the Government to render the conversation senseless by deleting all portions of the statements in the conversation made by the Senator.

The committee believes, however, that every effort should be made to minimize the "chilling effect" that retention of such conversations of Americans will have. Therefore, the definition of minimization procedures places additional restrictions on the dissemination of infor-

mation, where abuses are most likely to occur. These restrictions focus on those types of information which are the hardest to pin down concretely, that is, information which relates solely to the national defense or security and the conduct of foreign affairs. The bill requires procedures which are reasonably designed to insure that such information is not disseminated in a manner which identifies a U.S. person, without that person's consent, unless the person's identify is necessary to understand or assess the importance of information with respect to a foreign power of foreign territory or the information is otherwise publicly available.

The phrase "with respect to a foreign power or foreign territory" comes from the definition of "foreign intelligence information." It requires that the information must contribute to the fulfillment of the Government's requirements for foreign intelligence regarding foreign powers and territories.

The first part of this dissemination standard allows dissemination where a U.S. person's identity is "necessary to understand" information with respect to a foreign power or territory. 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. To take one obvious case, if the message says a foreign government official is arriving in this country at a particular time and place, it would be necessary to identify the airline he is arriving on. The airline company would fall in the definition of "United States person" if it is a U.S. corporation and not a foreign power.

Another 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 part of the special dissemination standard allows dissemination where a U.S. person's identity is necessary to "assess the importance" of information with respect to a foreign power or territory. The word "importance" means important in terms of the interests set out in the definition of foreign intelligence information. 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 asses that importance.

The third part of the special dissemination standard allows dissemination where the information identifying a U.S. person is otherwise publicly available. An example is a foreign official's discussion of the contents of a newspaper article referring to U.S. persons.

Of course, none of these are hard-and-fast lines. What the bill requires is careful deliberation by responsible officials in the executive branch. The court is also authorized to monitor compliance with the minimization procedures, including the special dissemination procedures, in order to deter abuses. There will inevitably be close judgment calls, both in devising detailed procedures and in applying them to particular circumstances. Therefore, the bill does not attempt to impose absolute rules, but rather says that the procedures must be "reasonably designed" to achieve their objectives.

S. 1566 as reported by the Judiciary Committee included different procedural requirements which had been added by this committee to S. 3197 in the 94th Congress. The committee has determined on the basis of further study that these procedures, dealing with the manner of retention of information and with surveillance of certain foreign-controlled entities, may be too complex to administer. Therefore, they have been deleted from the bill.

The committee looks with favor, however, upon efforts by the Executive Branch to devise and submit to the court more restrictive procedures than the minimum standards required by the terms of the bill itself. The Attorney General has already promulgated procedures governing certain surveillance activities which would be covered by S. 1566; and this committee has examined those procedures in the course of discharging its responsibilities. The committee does not intend that passage of S. 1566, which by its terms might be interpreted as permitting relaxation of current restrictions, should automatically have this effect.

In some instances the surveillance technology available to the Government requires more rigorous procedures than those prescribed by S. 1566, in order to safeguard privacy interests adequately. Such procedures cannot be spelled out by law, or otherwise disclosed publicly, without revealing sensitive sources and methods of foreign intelligence collection. Nevertheless, the committee intends that the Attorney General should continue the efforts already underway to establish procedures which will most effectively reconcile privacy interests with advancing technology, and that the court should take such considerations into account in approving the procedures that are proposed by the Attorney General. It is also anticipated that this committee will continue to review such procedures.

Existing policies governing the dissemination of information obtained through conventional electronic surveillance techniques, such as wiretapping, should be revised if they conflict with any requirement of the bill.[25] For example, information about the suitability or credibility of U.S. persons who are sources or contacts of an agency in the intelligence community, or who are reasonably believed to be potential sources or contacts, might be disseminated on specific request by name from the particular agency. It is questionable whether all such dis-

[25] C.F., letter from Attorney General Griffin B. Bell to Hon. Birch Bayh, chairman, Senate Select Committee on Intelligence, Feb. 28, 1978.

semination, without the person's consent, would be permitted as a routine matter under the minimization procedures of S. 1566. However, if the consent of the person is obtained for the conduct of an inquiry regarding his suitability or credibility as a source or contact, S. 1566 would allow such dissemination in the course of the inquiry. The person should be advised that consent for the inquiry means consent for the retrieval and dissemination of information in the possession of the agencies in the Intelligence Community by means, for example, of a "national agencies name check." Information may not, of course, be retained for such dissemination unless it otherwise satisfies the statutory requirements for retention.

Similarly, information might be disseminated where it raises a question about the trustworthiness of a current Federal employee, a former employee of an agency in the intelligence community, a person holding a security clearance or having access to sensitive information or facilities, or a person who held a security clearance for or was otherwise granted access to information classified as "Secret" or a higher classification. Such information might be disseminated to the Government employer or former employer, the agency which granted the clearance or access, or another Federal agency having responsibility to investigate the trustworthiness of the individual. Such dissemination might also occur where the information raises a question about the trustworthiness of individuals who are applicants or prospective Government employees, if the disseminating agency verified the employer's official interest in the individual concerned. Once again, it is questionable whether all such dissemination, without the person's consent, would be permitted as a routine matter; and information may not be retained for such dissemination unless it otherwise satisfies the requirements for retention.

The committee wishes to emphasize that dissemination without the person's consent requires a determination that the information relates to the ability of the United States to protect against grave hostile acts of a foreign power or foreign agent, sabotage or terrorism by a foreign power or foreign agent, or the clandestine intelligence activities of a foreign intelligence service or foreign agent; or that the information relates to national defense or security or foreign affairs and is necessary to understand or assess the importance of information with respect to a foreign power or territory or is otherwise publicly available.

A reasonable case can be made that information about the suitability or credibility of intelligence sources or contacts, and information about the trustworthiness of persons who hold, have held, or are expected to hold positions giving them access to sensitive information or facilities, would relate to the ability of the United States to protect against clandestine intelligence activities of a foreign power or foreign agent. The case is less compelling, however, where the information is not counterintelligence information but merely concerns the trustworthiness of a person who is a Government employee not having or having had access to sensitive information or facilities, or an applicant or prospective applicant for such a position.

Additionally, the provisions of S. 1566 permitting dissemination and use for law enforcement purposes of information that is evidence of a crime would not permit dissemination of information when nec-

essary to the conduct of any investigation that may be within the jurisdiction of a law enforcement agency. Such investigations must be criminal investigations, rather than civil, background, or other types of investigations.

If provision is made for dissemination in exceptional circumstances that are not otherwise provided for in more detailed minimization procedures, for example, with the prior approval of the Attorney General, such a provision must be approved by the judge to whom the procedures are presented in an application for an electronic surveillance order; and such a provision may be approved and applied only in conformity with the minimization requirements of S. 1566 itself.

These considerations should be taken into account by the court and by the executive branch, especially the Attorney General, in applying the minimization requirements of S. 1566 to the dissemination of information obtained through conventional electronic surveillance.

H. "United States person" and "United States"

Section 2521(b)(9) defines a "United States person" to include a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association of which a substantial number of members are citizens of the United States or permanent resident aliens, and a corporation incorporated in the United States, but not including corporations or associations which are "foreign powers" as defined in section 2521(b)(1)(A)–(E).

The term "United States person" was not defined in S. 3197, as reported in the 94th Congress, because S. 3197 made no distinction in its provisions between different types of "persons." S. 1566 does not, for example, afford to nonresident aliens the protections of the "minimization procedures" or the court's review of the certification that surveillance of the person is required to obtain information "necessary" for certain purposes. However, such protections either did not exist or were less stringent in S. 3197. Their application to nonresident aliens would impose undue burdens upon the court and the agencies conducting electronic surveillance.

The term "members" with respect to unincorporated associations 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 (B) and (E) 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."

S. 1566 as reported by the Judiciary Committee excluded from "United States person" any corporation or association which is a foreign power. This exception has been modified to exclude only those foreign powers which fall into parts (A)–(E) of the "foreign power" definition. A corporation incorporated in the United States, or an unincorporated association of which a substantial number of members

are American citizens or resident aliens, retains its "United States person" status if it is alleged to be directed and controlled by a foreign government, but where such direction and control is not openly acknowledged. This provides safeguards needed because of the possibility that such an entity could be placed under surveillance without meeting the requirements for surveillance of an individual U.S. person. See section 2521(b)(1)(E), supra.

Section 2521(b)(10) offers a new definition of "United States" for geographic purposes. Evidence publicized last year of CIA activities in Micronesia led the administration to propose this change which makes explicit that S. 1566 covers electronic surveillance in all areas under the territorial sovereignty of the United States (the United States and its territories) as well as the Canal Zone and Micronesia. The term "territorial sovereignty" does not include U.S. Embassies, military bases, and other installations abroad. The Commonwealth of the Northern Marianas is intended to be covered by this definition after its severance from the Trust Territory of the Pacific Islands. The remainder of the Trust Territory of the Pacific Islands is intended to be covered so long as the trust is in effect and thereafter only if the political status agreements with the United States provide for territorial sovereignty of the United States in a manner similar to that of the Northern Mariana Islands, Puerto Rico, or Guam.

Section 2522

Section 2522 authorizes the submission of applications to a judge for a court order approving the use of electronic surveillance under this chapter. Applications may be submitted only if the President has, by prior written authorization, empowered the Attorney General to approve the submission. This section does not require the President to authorize each specific application; he may authorize the Attorney General generally to seek applications under this chapter or upon such terms and conditions as the President wishes so long as the terms and conditions are consistent with this chapter. 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 S. 1566. The procedures of this bill are "the exclusive means" by which electronic surveillance, as defined in section 2521(b)(6), may be conducted. See conforming amendment section (f) to section 2511(2), chapter 119, United States Code, infra. This bill will establish the exclusive United States law governing electronic surveillance in the United States for foreign intelligence purposes. Therefore, an application for a court order which meets the standards of this bill should be granted, notwithstanding any other law, treaty, or international agreement.

Section 2523

Subsection (a) provides for public designation by the Chief Justice of seven U.S. district court judges to sit on a special court, each member of which may hear applications and grant orders under this chapter. The court shall have nationwide jurisdiction, and the committee contemplates that there will be some geographic dispersion among the judges designated. The provision for the judges to serve as members of a special court has been added upon the recommenda-

tion of the General Counsel of the Administrative Office of the U.S. Courts.[26] The committee intends that the special court should sit continuously in the District of Columbia.

The subsection provides that none of the designated judges shall have jurisdiction to hear an application for electronic surveillance if that same application has been previously denied by another of the designated district judges. This provision is intended to make clear that if the Government desires to pursue an application after a denial, it must seek review in the special court of review established in subsection (b); it cannot apply to another district judge. Obviously, where one judge has asked for additional information before approving an application, and that judge is unavailable when the Government comes forward with such additional information, the Government may seek approval from another judge. It would, however, have to inform the second judge about the first application. See section 2524(a)(9), infra.

Similarly, where an application is made and then withdrawn, perhaps because a change in circumstances makes the electronic surveillance no longer technically feasible, the Government may seek approval from another judge if the application is subsequently reinstated. The committee does not intend, however, that the Government be allowed to seek approval from another judge if the original withdrawal was occasioned by indications that the first judge intended to deny or modify the order requested by the Government.

The subsection further provides that a designated district judge who denies an application for electronic surveillance shall provide a complete written statement of the reasons for the denial, and, if the Government seeks review of the decision, forward that statement and other documents comprising the record to the special court of review. This insures that the special court of review will have the full record of the proceedings of the district court in reviewing the case.

Subsection (b) provides for the public designation by the Chief Justice of three judges from the Federal courts of appeals or district courts who shall sit together as a special court of review having jurisdiction to review denials of applications made to the individual judges designated in subsection (a). One of the three is to be designated publicly as the presiding judge. If the special court of review determines that an application was properly denied, it shall provide a wrtten statement of the reasons for its decision and, on petition of the Government for a writ of certiorari, forward the complete record to the Supreme Court, which will have jurisdiction to review the decision.

Subsection (c) provides for the expeditious handling of all proceedings under this chapter and also states that the Chief Justice, in consultation with the Attorney General and the Director of Central Intelligence, shall establish security measures under which applications made and orders granted shall be maintained. The committee contemplates that the record of applications made, information provided, and orders granted by the several judges designated under this chapter shall be maintained in such a way that the judges designated

[26] 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, Jan. 10, 1978.

under this chapter shall have access when necessary to the records of actions taken by the other judges similarly designated.

Subsection (d) has been added to S. 1566, as reported by the Judiciary Committee, for the purpose of providing fixed, staggered terms for the judges, also as recommended by the General Counsel of the Administrative Office of the U.S. Courts. Each judge designated under this section shall so serve for a maximum of 7 years and shall not be eligible for redesignation. The judges first designated under subsection (a) shall be designated for terms of from 1 to 7 years so that one term expires each year. The judges first designated under subsection (b) shall be designated for terms of 3, 5, and 7 years.

Section 2524

This section is patterned after 18 U.S.C. section 2518 (1) and (2), and specifies what information must be included in the application. Applications must be made 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 the investigating officer personally attesting to the status and reliability of any informants or other covert sources of information. By this means the source of all information contained in the application and its accuracy will have been sworn to by a named official of the 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 an agent of a foreign power and that the facilities or place at which the electronic surveillance is directed are being used, or about to be used, by an agent of a foreign power, and that all other statutory criteria have been met. In addition, the Attorney General must personally be satisfied that the certification 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 of the applicant to make this application. This would consist of the Presidential authorization to the Attorney General and the Attorney General's approval of the particular application.

Paragraph (3) requires the identity or description of the person who is the target of the electronic surveillance. The word "person" is used in its juridical sense to mean the individual or entity that is the target of the surveillance. However, care must be taken in framing the order authorizing such surveillance—and minimization procedures—

that surveillance against one individual does not lead to the acquisition, retention, and dissemination of communications of an entire group or organization of U.S. citizens, thus violating constitutional rights of association and privacy.

Paragraph (4) requires a statement of the facts and circumstances justifying the applicant's belief that the target of the electronic surveillance is a foreign power or an agent of a foreign power and that the facilities or place at which the surveillance is directed are being used or are about to be used by that power or agent. These requirements parallel existing law 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 subject to close judicial review. These procedures may differ from case to case, depending on the type of foreign agent involved, the individuals using the facilities or place to be surveilled, the type of foreign intelligence information sought, and other similar factors. Minimization procedures should where possible include such elements as methods to avoid the acquisition of irrelevant information at the time of intercept, restrictions on the use of surveillance to times when foreign intelligence information is likely to be obtained, and requirements for deletion of information obtained which does not relate to foreign intelligence purposes.

For example, steps should be taken to prevent unnecessary invasion of the privacy of a target's family caused by a 24-hour tap on the family phone when it is known that the target is out of town or at the office. Similarly, conversations unrelated to foreign intelligence should not be retained or, of course, disseminated.

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 indentical concerns with respect to protecting U.S. persons' rights. This is so regardless of the specific targets involved and 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, except where the surveillance is of a foreign power as defined in section 2521(b)(1)(A), (B), or (C). The description should be as specific as possible and sufficiently detailed so as to state clearly what the Government seeks. A simple designation of which subdefinition of "foreign intelligence information" is involved will not suffice. Such a description is not required where a target is one of the "official" foreign powers defined in section 2521 (b)(1) (A), (B), or (C). Where these types of powers are the targets, a designation of a particular subcategory of the definition of "foreign intelligence information," as required by subparagraph (7)(D), will suffice. The reason for this distinction is that, with respect to such "official" targets, the sensitivity of the surveillance

is greatly multiplied while the risk of a fruitless surveillance which will not obtain any foreign intelligence information is greatly reduced. Therefore the administration maintains that such applications should not require as much detailed information to be presented as in cases involving American citizens or other individual targets.

Paragraph (7) requires a certification or certifications by the Assistant to the President for National Security Affairs or by an 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 for the collection of the information—normally the Assistant to the President for National Security Affairs, the Director of Central Intelligence, the Director of the Federal Bureau of Investigation, or the Secretary of Defense—or such other officer, appointed with the advice and consent of the Senate, who has full knowledge of the case. The possibility of additional certifications 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 (c) and section 2525(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 of what type of foreign intelligence information is sought and, where the target is not a foreign power as defined in section 2521(b)(1) (A), (B), or (C), 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, where the target is not a foreign power as defined in section 2521 (b)(1) (A), (B), or (C), 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 certification 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 one individual for electronic surveillance when the true purpose of the surveillance is to gather information about another individual. It is also designed to make explicit that the sole purpose of such surveillance is to secure foreign intelligence information and not to obtain information for any other purpose. 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.

Finally, where the target of the surveillance is one of the special class of "official" foreign powers (defined in sections 2521(b)(1)(A), (B), or (C)), the certification shall include a statement of the period of time for which the surveillance is required. With respect to surveillances of this special class of foreign powers, this statement is placed in the certification because the reviewing court does not have the power to control the length of the surveillance as is the case within the 90-day period otherwise applicable in the bill.

Paragraph (8) requires the application to contain a statement of the means by which the surveillance will be effected where the target is other than the special class of foreign powers. Where the target is one of the special classes of foreign powers listed in section 2521(b)(1)(A), (B), or (C), only a designation of the type of surveillance according to the categories of the definition of electronic surveillance is required. It will be sufficient in such cases if the application merely indicates whether the information will be acquired by means of a wiretap, a microphone installation, the interception of a radio signal, or some other means. Less specificity in describing the means of the surveillance is required for the special class of foreign powers because of the extreme importance and sensitivity of the information sought. If such a surveillance requires physical entry (whether forcible or not) of the property of a nonconsenting person, a statement to that effect is required.

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 in those cases where the special class of foreign powers is not the target. 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.

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

Subsection (c) enables the judge to require the applicant to furnish further information as may be necessary to make the 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 2525

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 special class of foreign powers is the target) or the minimization proce-

dures 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 the facilities or place at which the surveillance is directed are being used or are about to be used by that power or agent.

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

In addition, in order to find "probable cause" to believe the subject of the surveillace is an "agent of a foreign power" under subsection 2521(b)(2), 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 2521(b)(1). There must also be probable cause to believe the person is acting for 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, terrorism, or other proscribed activities as defined in section 2521(b)(2)(B).

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, terrorism, or clandestine intelligence activities at the direction of a foreign power.

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. citizens or lawful resident alien fit the definition of minimization procedures. The committee contemplates that the court would give these procedures most careful consideration. If it is not convinced that they will be effective, the application should be denied or the procedures modified. The committee realizes that total minimization may not be possible. Therefore, the bill's requirement is phrased in terms of minimization procedures being "reasonably designed." Thus, for example, where irrelevant information cannot be erased from part of a tape, minimization procedures should restrict dissemination of the tape. In addition, where it cannot be determined immediately whether

a certain piece of information is irrelevant, minimization procedures should require that within a specified time such a determination be made and the irrelevant matter expunged.

Paragraph (5) requires that the judges find that the application contains the description and certification or certifications specified in section 2524(a)(7). If the application meets the requirements of those sections, 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. This authority of the court to "look behind" the certification for surveillances of Americans and reject them if "clearly erroneous" is recognized by the committee as a major improvement over S. 3197 (which did not provide for any judicial review of the certifications). The "clearly erroneous" standard of review is not, of course, comparable to a probable cause finding by the judge. Nevertheless, S. 1566 does provide a workable procedure for judicial review (and possible rejection) of executive branch certifications for surveillances of United States persons.

S. 1566 as reported by the Judiciary Committee 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 2524(c) supra. The judge must find that the determination by the certifying official that the 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 of whether probable cause exists that the target of surveillance is a foreign power or its agent. Second, the certification procedure assures written accountability within the executive branch for the decision made to engage in such surveillance. This constitutes an internal check on executive branch arbitrariness.

Moreover, it should be noted that if the description and certification do not comply fully with section 2524(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 be obtained through normal investigative techniques, the judge could (if surveillance was not targeted against the special class of foreign powers) 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 or a description of the person or persons targeted by the electronic surveillance. The order must specify the place or facilities against which the surveillance is directed. The order must also specify the type of information sought, or where the special class of foreign powers is the target, the specific category of "foreign intelligence information." These requirements are designed to satisfy the fourth amendment's requirements that warrants describe with particularity and specificity the person, place, and objects to be searched or seized. The order must, in addition to the fourth amendment's requirements, specify the means by which the surveillance will be effected (where the target is one of the special class of foreign powers, however, only the specific category of "electronic surveillance" is required). In addition, the order must specify the period of time during which the surveillance is approved.

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

The order may also direct that a common carrier, landlord, custodian, contractor or other specified person furnish information, facilities or technical assistance necessary to accomplish the electronic surveillance successfully and with a minimum of interference to the services provided by such person to the target of the surveillance. If 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 section 4(b) of this bill. That amendment requires that before a communication common carrier or its agent provides such information, facilities or technical assistance to an investigative or law enforcement officer, that officer is required to furnish to the carrier either an order signed by the authorized judge certifying that a court order directing such assistance has been issued or, in the case of surveillance undertaken under chapter 119 or 120 in which a prior order is not required, such as an emergency surveillance, a certification under oath by the officer requesting the assistance that the applicable statutory requirements have been met.

Subsection (c) allows an order approving electronic surveillance under this chapter against any person or entity other than a special foreign power as defined in section 2521(b)(1)(A), (B), or (C) 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.[27]

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. As already indicated, this is a substantial change from S. 3197 as reported in the 94th Congress. There are, however, considerable arguments for the change: First, the determination that an entity is within the definition of section 2521(b)(1) (A), (B), or (C) 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 generation of four times the amount of required paperwork with the attendant increased possibility of a 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.

In coming to this conclusion, however, the committee emphasizes that, in order for U.S. citizens to be protected adequately in such cases, this provision must not be interpreted to bar judicial review of the effectiveness of the minimization procedures. U.S. citizens may be overheard talking to employees of such an "official" foreign power or may be referred to by such employees. As already indicated, the court has the power to review minimization during the course of the surveillance as it does now under chapter 119. This applies regardless of the type of target and remains an important protection.

As under chapter 119, extensions of an order may be sought and granted on the same basis as the original order. A new application, including a new certification pursuant to section 2524(a)(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. To aid the judge in making this determination anew, it is expected that the court would evaluate the success or failure of any previous surveillances and the facts and circumstances surrounding such surveillance. The court, however, in considering a renewal involving a foreign power as defined in section 2521(b)(1) (A), (B), or (C), cannot order the Government to submit any information actually obtained as a result of the original surveillance or previous extension. This change from S. 3197 reflects concern with the sensitive nature of the information obtained from special foreign powers.

---

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

In order to make clear the judge's authority to review compliance with the minimization procedures, a provision has been added at the end of subsection (c). 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 required by this chapter. This provision is not intended to require the judge to 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 that 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 2521(b)(1)(A), (B), or (C).

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

The procedures under which such an emergency surveillance is authorized are considerably stricter than those of the comparable provision in chapter 119, 18 U.S.C. 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 chapter for the issuance of a judicial order be followed during the period of the emergency surveillance. There is no comparable provision under 18 U.S.C. 2518(7). 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 could 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 chapter will receive judicial review and that judicial approval or denial will be forthcoming nunc pro tunc. Thus, the termination of an emergency surveillance before the expiration of the 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 2523, following the denial of an application for a judicial order. Under such circumstances, the Attorney General could not reasonably determine that the factual basis for the issuance of an order under this chapter to approve such surveillance exists, as required by this subsection.

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

S. 1566 as reported by the Judiciary Committee did not cover the use of information acquired from such disapproved emergency surveillance for other purposes. Further restrictions are needed so that there is less incentive to use questionable emergency surveillances. The additional provision requires that no information concerning any U.S. person acquired from a disapproved emergency 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 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 2523.

Section 2526

This section sets forth the permissible uses which may be made of information acquired by means of electronic surveillance conducted pursuant to this chapter. The fact that effective minimization with regard to acquisition and retention may be more difficult in the foreign intelligence area than in the more traditional criminal area, and that this chapter contains certain less restrictive procedures than does chapter 119—for example, 90 days or 1 year of surveillance per order rather than 30 days—mandates that the uses to be made of the information acquired by means of this chapter be carefully restricted.

This section, therefore, places more stringent restrictions on dissemination and use than does the corresponding provision of title III, 18 U.S.C. 2517. The extent to which the Government should be required to surrender to the parties in a criminal trial the underlying documentation used to justify electronic surveillance raises delicate problems and competing interests. On the one hand, broad rights of access to the documentation and subsequent intelligence information can threaten the secrecy necessary to effective intelligence practices. However, the defendant's constitutional guarantee of a fair trial could be seriously undercut if he is denied the materials needed to present a proper defense. The committee believes that a just, effective balance has been struck in this section.

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

In order to make clear that this provision is linked directly to the required minimization procedures, one addition has been made to S. 1566 as reported by the Judiciary Committee. Information must not only be used or disclosed for the specified purposes, but it must also be used and disclosed in accordance with the minimization procedures required by this chapter.

A major change from S. 3197 has been made in this section at the insistence of the administration. Whereas in S. 3197 this section applied to all persons, regardless of whether they were Americans, S. 1566 limits the protections of section 2526(a) to U.S. persons. Information concerning non-U.S. persons—who indeed may be foreigners not even in the United States—is not subject to the same restrictions as information concerning U.S. persons. For example, the information obtained might be used to deport an illegal alien even though such use of the information is not for foreign intelligence purposes and is not for the purpose of enforcing the criminal law.

This differentiation between U.S. persons and other persons was sufficiently troublesome to result in an important Judiciary Committee amendment to section 2526(a). By limiting the subsection to U.S. persons, the possibility existed that information obtained by surveillance could be used in a variety of illegal ways against, for example, foreign visitors and students. The Judiciary Committee amended this subsection to make clear that no information acquired pursuant to this chapter may be used or disclosed for other than lawful purposes. The bill does not permit information gathered about the lawful activi-

ties or private life of a foreign visitor to be used to illegally blackmail him into becoming an agent against his country. S. 1566, as amended, now requires that in those cases where the Government wishes to use foreign intelligence information against non-U.S. persons beyond the specific purposes listed in section 2526(a), it do so in a lawful manner and for lawful 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 chapter—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 chapter were to overhear information relating to a violation of State criminal law, such as homicide, the agents could hardly be expected to conceal such information from the appropriate local officials. Second, the committee can conceive of situations where disclosure should be made outside of 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 chapter 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.

Section 2526(a) also states that foreign intelligence information obtained may be used to enforce the criminal law if its use outweighs the possible harm to the national security. This new language, which did not appear in S. 3197, states the obvious. The Department of Justice always has the option of deciding whether to proceed with a criminal prosecution or forego it in the interests of national security. For example, the Department of Justice may decline to prosecute rather than disclose the names of important witnesses and key informants. Whether to go forward with a criminal prosecution remains in the exclusive hands of the executive branch and nothing in section 2526(a) changes that fact. This provision should under no circumstances be interpreted to deny the Attorney General the opportunity to perform his important role in this weighing of interests.

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

Subsection (b) must be read in conjunction with the minimization requirements of section 2521(b)(8) and with the preceding subsection (a). As previously noted, the minimization procedures mandated by the court are designed to restrict the acquisition of information obtained by means of electronic surveillance to information related to foreign intelligence. However, even the most thorough minimization efforts may result in the acquisition of some information which is not foreign intelligence information. This subsection states that the minimization procedures required by this chapter do not preclude the retention and dissemination of any information which is evidence of a crime. Such disclosure would, of course, be restricted by the provisions of subsection (a).

The implication that such criminal evidence be acquired incidentally logically connotes that it must be acquired lawfully. This requires that there be a good faith effort to minimize.[28] Thus for example, if monitoring agents choose to disregard the minimization standards and thereby acquire evidence of a crime against an overheard party whose conversation properly should not have been acquired, that evidence would be acquired in violation of this chapter and would properly be suppressed if offered at any official proceeding. See subsection (c), infra.

Disclosure 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 the evidence the Attorney General would alert the prosecutor to the surveillance and he, in turn, would alert the court in accordance with subsection (c).

---

[28] *United States* v. *Armocida*, 515 F. 2d 29 (3d Cir. 1975).

Subsections (c), (d), and (e) 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 will not 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 subsection (c) abrogates the rights afforded a criminal defendant under *Brady* v. *Maryland*,[29] and the Jencks Act.[30] 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.[31]

Subsection (c) states that no information acquired pursuant to this chapter may be used unless, prior to the trial, hearing, or other proceeding, or at a reasonable time prior to an effort to disclose the information or submit it in evidence, the Government notifies the court that such information was acquired by means of electronic surveillance conducted pursuant to this chapter. This provision has been broadened in S. 1566 over its counterpart in S. 3197 by including nonjudicial proceedings. In instances in which the Government intends to disclose surveillance information in such a nonjudicial forum, subsection (c) would require that the U.S. district court in the district in which the disclosure is to take place be notified of the proposed disclosure or use.

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

The "subject" of electronic surveillance means an individual who was a party to a communication acquired by electronic surveillance or was a person against whom the surveillance was directed. Thus the word would include an "aggrieved person" as defined in section 2510 of title III.[32]

One situation in which such motion might be presented would be that in which the court orders disclosed to the party the court order and accompanying application under subsection (e) prior to ruling on the legality of the surveillance. Such motion would also be appropriate, however, even after the court's finding of legality if, in sub-

[29] 373 U.S. 83 (1963).
[30] 18 U.S.C. 3500 et seq
[31] *United States* v. *Andolschek*, 142 F. 2d 503 (2nd Cir. 1944).
[32] See also, *Alderman* v. *United States*, 394 U.S. 165 (1967).

sequent trial testimony, a Government witness provides evidence that the electronic surveillance may have been authorized or conducted in violation of the court order. The most common circumstance in which such a motion might be appropriate would be a situation in which a defendant queries the Government under 18 U.S.C. 3504 and discovers that he has been intercepted by electronic surveillance even before the Government has decided whether evidence derived from that surveillance will be used in the presentation of its case. In this instance, under the appropriate factual circumstances, the defendant might move to suppress such evidence under this subsection even without having seen any of the underlying documentation.

A motion under this subsection shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the movant was not aware of the grounds for the motion. The only change in subsection (d) from S. 3197 is to remove as a separate, independent basis for suppression the fact that the order was insufficient on its face. This is not a substantive change, however, since communications acquired pursuant to an order insufficient on its face would be unlawfully acquired and therefore subject to suppression under paragraph (1).

Subsection (e) states in detail the procedure the court shall follow when it receives a notification under subsection (c) or a suppression motion is filed under subsection (d). This procedure applies, for example, whenever an individual makes a motion pursuant to subsection (d) or 18 U.S.C. 3504, or any other statute or rule of the United States to discover, obtain or suppress evidence or information obtained or derived from electronic surveillance conducted pursuant to this chapter (for example, Rule 12 of the Federal Rules of Criminal Procedure). Although a number of different procedures might be used to attack the legality of the surveillance, it is this procedure "notwithstanding any other law" that must be used to resolve the question. The committee wishes to make very clear that the procedures set out in subsection (e) apply whatever the underlying rule or statute refered to in the motion. This is necessary to prevent the carefully drawn procedures in subsection (e) from being bypassed by the inventive litigant using a new statute, rule or judicial construction.

The special procedures in subsection (e) cannot be invoked until they are triggered by a Government affidavit that disclosure or an adversary hearing would harm the national security of the United States. If no such assertion is made, the committee envisions that mandatory disclosure of the application and order, and discretionary disclosure of other surveillance materials, would be available to the defendant, as is required under title III. When the procedure is so triggered, however, the Government must make available to the court a copy of the court order and accompanying application upon which the surveillance was based.

The court must then conduct an ex parte, in camera inspection of these materials as well as any other documents relation to the surveillance which the Government may be ordered to provide, to determine whether the surveillance was authorized and conducted in a manner which did not violate any constitutional or statutory right of the person against whom the evidence is sought to be introduced. The sub-

section 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 make an accurate determination of the legality of the surveillance.

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

> Moreover, we did not in *Alderman*, *Butenko* or *Ivanov*, and we do not today, specify the procedure that the district courts are to follow in making this preliminary determination [of legally.]

394 U.S. 310, 314 (1968); see also, *Taglianetti* v. *United States*, 394 U.S. 316 (1968). The committee views the procedures set forth in this subsection as striking a reasonable balance between an entirely in camera proceeding which might adversely affect the defendant's ability to defend himself, and mandatory disclosure, which might occasionally result in the wholesale revelation of sensitive foreign intelligence information.

The decision whether it is necessary to order disclosure to a person is for the Court to make after reviewing the underlying documentation and determining its volume, scope, and complexity. The committee has noted the reasoned discussion of these matters in the opinion of the Court in *United States* v. *Butenko*, *supra*. There, the Court, faced with the difficult problem of determining what standard to follow in balancing national security interests with the right to a fair trial, stated:

> The distinguished district court judge reviewed in camera the records of the wiretaps at issue here before holding the surveillance to be legal * * *. Since the question confronting the district court as to the second set of interceptions was the legality of the taps, not the existence of tainted evidence, it was within his discretion to grant or to deny Ivanov's request for disclosure and a hearing. The exercise of this discretion is to be guided by an evaluation of the complexity of the factors to be considered by the court and by the likelihood that adversary presentation would substantially promote a more accurate decision. (494 F. 2d at 607.)

Thus, in some cases, the Court will likely be able to determine the legality of the surveillance without any disclosure to the defendant. In other cases, however, the question may be more complex because of, for example, indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order. In such cases, the committee contemplates that the court will likely decide to order disclosure to the defendant, in whole or in part, since such disclosure "is necessary to make an accurate determination of the legality of the surveillance." [33]

---

[33] Cf. *Alderman* v. *United States*, 394 U.S. 165, 182 n. 14 (1968); *Taglianetti* v. *United States*, supra at 317.

Cases may arise, of course, where the Court believes that disclosure is necessary to make an accurate determination of legality, but the Government argues that to do so, even given the Court's broad discretionary power to exercise certain sensitive portions, would damage the national security. In such situations the Government must choose—either disclose the material or forgo the use of the surveillance-based evidence. Indeed, if the Government objects to the disclosure, thus preventing a proper adjudication of legality, the prosecution would probably have to be dismissed, and, where the Court determines that the surveillance was lawfully authorized or conducted, the court would, "in accordance with the requirements of law," suppress that evidence which was unlawfully obtained.

The committee has chosen the general phrase "in accordance with the requirements of law" to deal with the problem of what procedures are to be followed in those cases where the trial court determines that the surveillance was unlawfully authorized or conducted. The evidence obtained would not, of course, be admissible during the trial. But beyond this, in the case of an illegal surveillance, the Government is constitutionally mandated to surrender to the defendant all the records of the surveillance in its possession 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 confidential materials 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.)

Where the court determines 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, a motion for discovery of evidence must be denied unless disclosure or discovery is required by due process.

Subsection (f) 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 forgo 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 had focused an investigation on the target. Even where the target is not, in fact, an agent of a foreign power, giving notice to the person may result in compromising an 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.

A new subsection (g) has been added to S. 1566 as reported by the Judiciary Committee, 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 section 2521(b)(6)(C) 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 person 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.

Section 2527

Section 2527 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 chapter. 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 chapter is used.

The requirements in S. 3197 for the public reporting of certain additional statistics have been altered due to the introduction in S. 1566 of two different types of warrant (creating a 90-day warrant for one class of target, and a 1-year warrant for official foreign powers). The reporting requirements in S. 3197, if reenacted verbatim in S. 1566, would obviously give foreign intelligence networks significant information concerning the number and duration of surveillances of official foreign powers. Changes have been made, therefore, in the public reporting requirements of S. 3197 so as to avoid the compromising of sensitive information. The statistics reported pursuant to this section may be made public.

Section 2528

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, unlike the statutory provisions of title III of the Omnibus Crime Control Act of 1968, it is not contemplated that most electronic surveillance conducted pursuant to this chapter 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 2528 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 chapter. He must do so at least semiannually.

The use of the word "fully" in this provision has the meaning used in Senate Resolution 400, 94th Congress, 2nd session, which expresses the sense of the Senate that the head of each department and agency of the United States should keep the Select Committee on Intelligence "fully and currently informed with respect to intelligence activities, including any significant anticipated activities, which are the responsibility of or engaged in by such department or agency." A similar provision appears in Executive Order 12036, January 24, 1978. This requirement does not constitute a condition precedent to the implementation of any such anticipated intelligence activity. As interpreted by the committee, the "fully" requirement means that the committee must be given enough information to understand the activities, 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. To preserve the committee's right to seek further information, when necessary, section 2528 adopts language similar to that contained in S. 3197 as reported in the 94th Congress. It makes clear that nothing in this chapter shall be deemed to limit the authority and responsibil-

ity 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 Senate Select Committee on Intelligence, that authority and responsibility is set forth in Senate Resolution 400, 94th Congress, 2d session.

Section 2528 also incorporates a provision contained in S. 3197 requiring the Senate Select Committee on Intelligence to report each year to the Senate concerning the implementation of this chapter. It also provides that any amendments to this chapter proposed by the committee shall be considered and acted upon promptly.

In the exercise of their respective functions, the Senate Select Committee on Intelligence and the Senate Committee on the Judiciary shall consult with members of the Department of Justice and the intelligence community concerning the proper implementation of the act.

Section 3

Section 3 delays the effective date of the act until 90 days following the designation of the first judge pursuant to section 2523 of this chapter. The purpose of this delay is to allow time for the development of the applications required under this bill and of security measures governing the submission of these applications to the courts. The 90-day delay will also prevent the situation where one judge will be forced to handle all of the applications.

CONFORMING AMENDMENTS

Section 4 serves the important purpose of integrating the new chapter 120 with the current electronic surveillance law found in chapter 119 of title 18, United States Code. Various provisions of chapter 119 are applicable to the electronic surveillance engaged in under the new bill and the conforming amendments in this section of S. 1566 are designed to make changes reflecting this fact. In addition, where certain provisions of chapter 119 should not encompass the surveillance procedures in S. 1566, conforming amendments so limit such sections:

(a) (1) and (2). These amendments are designed to establish the same criminal penalties for violations of this chapter as apply to violations of chapter 119. As amended, these sections will make it a criminal offense to engage in electronic surveillance except as otherwise specifically provided in chapters 119 and 120. This amendment also provides, however, that "with respect to techniques used by law enforcement officers" which do not involve the actual interception of wire or oral communications, yet do fall within the literal definition of electronic surveillance in chapter 120—such as the use of a pen register—the procedures of chapter 120 do not apply. In such cases criminal penalties will not attach simply because the Government fails to follow the procedures in chapter 120 (such penalties may, of course, attach if the surveillance is commenced without a search warrant or in violation of a court order). In all cases involving electronic surveillance for the purpose of obtaining foreign intelligence information, however, the prohibitions of 18 U.S.C. 2511 would apply.

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

The statute calls for a fine of not more than $10,000 or imprisonment for not more than 5 years, or both, for each violation.

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

(b)(2). This amendment, when read in conjunction with section 2525(b)(2)(B), makes explicit the fact that a court order obtained under chapter 120 may direct an officer, employee or agent of a communication common carrier to provide certain assistance to the Government agents implementing the order. The nature and scope of such assistance is intended to be identical to that which may be directed under section 2518(4)(e) of chapter 119. The amendment further provides that before the carrier may provide such information or assistance, whether under chapter 119 or 120, the Government agent must furnish the carrier with an order signed by the court (but not necessarily the same order as authorizes the actual surveillance) if an order has been acquired, or a sworn statement by the agent that all statutory requirements have been met if the surveillance is being conducted pursuant to the provisions of section 2518(7) of chapter 119 or section 2525(d) of chapter 120. The document so furnished must also set forth the period of time for which the surveillance is authorized and a description of the facilities from which the communication is to be intercepted. And violation of this subsection by a carrier or its representative will render the carrier liable for the civil damages provided for in section 2520, subject, of course, to the good faith reliance defense contained therein.

At the request of the administration, the committee has added a provision to regulate the practice of any telephone company to inform customers who request a line check whether or not there is a wiretap on their line. It provides that no communication common carrier or officer, employee, or agent thereof shall disclose the existence of any interception under chapter 119 or any electronic surveillance, as defined in chapter 120, with respect to which the common carrier has been furnished either an order or certification under this subparagraph, except as may otherwise be lawfully authorized. The ban upon disclosure is intended to include disclosure of the existence of the electronic, mechanical, or other device used to accomplish any such interception or surveillance. This provision is not intended to bar disclosure to another officer, employee, or agent of a common carrier, where properly authorized by that common carrier.

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

(c)(2). This amendment makes clear that it is legal to engage in

electronic surveillance, as well as intercept a wire or oral communication, if a party consents.

(c)(3). This amendment: (1) provides statutory authorization for the Government to conduct tests of equipment which may result in electronic surveillance as defined in section 2521(b)(6); (2) authorizes the conduct of "sweeps" to discover illegal taps and bugs, which "sweeps" may result in "electronic surveillance" as defined in section 2521(b)(6); and (3), makes explicit that chapters 119 and 120 are "exclusive means by which electronic surveillance, as defined in section 2521(b)(6) of chapter 120, and the interception of domestic wire and oral communications may be conducted."

An additional provision has been inserted to require that all such testing and defensive "sweeps" be conducted under procedures approved by the Attorney General. Such a requirement has already been established by the President for activities conducted by any agency of the intelligence community, Executive Order 12036, January 24, 1978.

All tests conducted pursuant to this provision must be in the normal course of official business by the Government agent conducting the test and must be designed solely for determining the capability of equipment used for foreign intelligence gathering purposes. In addition, the test period shall be limited to that necessary to determine such capability and shall in no instance exceed 90 days without the express approval of the Attorney General. The contents of any communication acquired as a result of the test shall be disclosed only to those officials conducting the test and shall be used and retained by them only for the purpose of the test. At the completion of the testing period, the contents so acquired shall be destroyed. No particular U.S. person may be intentionally targeted for testing purposes without his consent.

The committee contemplates that in all cases such testing will be approved by a senior official prior to the commencement of the testing period.

"Sweeps" to discover the existence and capability of electronic surveillance equipment in violation of 18 U.S.C. 2511 or 47 U.S.C. 605 do not have a specific time limit, but are limited in time to that "necessary to determine the existence and capability of such equipment."

The Department of Defense, in a letter to the Judiciary Committee, has characterized these activities as follows:

> These activities, commonly called technical surveillance countermeasures surveys, are for the purpose of determining if a particular sensitive area has been penetrated by electronic surveillance devices installed by a foreign power or other hostile forces. In some cases, these surveys are conducted on a continuous basis. Since these activities are strictly defensive in nature and are for the sole purpose of detecting and neutralizing the illegal efforts of hostile powers, a time limit does not seem appropriate.

Information acquired pursuant to such "sweeps" may be used only to enforce chapter 119 or section 605 of the Communications Act of 1934, or to protect information from being subject to unlawful electronic surveillance. The provision is not an authorization to target

a person known to be, or suspected of, engaging in unlawful electronic surveillance, even where the purpose is to determine the existence and capability of that person's electronic surveillance equipment. If the person engaged in the unlawful electronic surveillance is an agent of a foreign power, he should be targeted under the applicable provisions of chapter 120. This provision is designed to confer statutory authority on the Government's effort to locate and analyze unlawful electronic surveillance activity.

A new paragraph (f) is added to section 2511(2) by this conforming amendment, which must be read in conjunction with the conforming amendment contained in paragraph (d) which repeals section 2511(3) of title 18, United States Code, the so-called national security disclaimer of title III of the 1968 Omnibus Crime Control and Safe Streets Act. The effect of these two conforming amendments is to establish chapter 120 as the exclusive congressional statement on the question of the Executive's power to order electronic surveillance.

This new paragraph states that nothing 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 chapter 120. The purpose of this prefactory phrase is twofold. First, it sets forth the sections of the United States Code which regulate the procedures by which electronic surveillance may be conducted within the United States and the statutory controls for the use and dissemination of information so acquired. If enacted, this chapter will constitute the sole and exclusive statutory authority under which electronic surveillance of a foreign power or its agent to obtain foreign intelligence information may be conducted within the United States. It will complement chapter 119, which deals with electronic surveillance for law enforcement purposes, and section 605 of the Communications Act of 1934, as amended, which restricts the dissemination of certain information transmitted by wire or radio. Second, the language of this amendment exempts from section 605 and chapter 119 foreign intelligence gathering from international or foreign communications by means of an electronic, mechanical, or other surveillance device if the acquisition does not come within the definition of "electronic surveillance" contained in section 2521(b)(6). Specifically, this provision is designed to make clear that the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States. As to methods of acquisition which come within the definition of "electronic surveillance" in this bill, the Congress has declared that this statute, not any claimed Presidential power, controls.

Paragraph (f) continues by stating that with respect to electronic surveillance, as defined in section 2521(b)(6), and the interception of domestic wire and oral communications, the procedures of chapters 119 and 120 shall be the "exclusive means by which electronic surveillance * * * and be * * * conducted." This statement puts to rest the notion that Congress recognizes an inherent Presidential power to conduct such surveillances in the United States outside of the procedures contained in chapters 119 and 120.

Article I, section 8, of the Constitution states:

> The Congress shall have Power * * * To make all laws which shall be necesary 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 explicitly rejected seizure of the steel mills and enacted a legislative alternative to curb labor unrest. In his concurring opinion, Justice Jackson wrote:

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

(d) This amendment repeals section 2511(3) of chapter 119, thereby eliminating any congressional recognition or suggestion of inherent Presidential power with respect to electronic surveillance.

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

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

(g) This amendment makes explicit that the necessary elements of an order set forth in subsection 2518(4) apply only to surveillance conducted pursuant to chapter 119, since chapter 120 contains its own requirements.

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

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

(j) This amendment makes explicit that the reporting requirements of the Administrative Office of the U.S. courts contained in this sub-

section apply only to surveillances conducted pursuant to chapter 119 since chapter 120 contains its own requirements.

(k) These amendments are designed to authorize the recovery of civil damages for violations of chapter 120 in the same manner and amounts as already provided for violations of chapter 119. The only category of individuals who would be exempted from the provisions of this section are foreign powers and agents of a foreign power as defined in section 2521(b)(1) and (b)(2)(A) of chapter 120.

CONGRESSIONAL BUDGET OFFICE,
U.S. CONGRESS,
Washington, D.C., March 14, 1978.

Hon. BIRCH BAYH,
Chairman, Select Committee on Intelligence,
U.S. Senate, Washington, D.C.

DEAR MR. CHAIRMAN: Pursuant to section 403 of the Congressional Budget Act of 1974, the Congressional Budget Office has reviewed S. 1566, the Foreign Intelligence Surveillance Act of 1977, as ordered reported by the Senate Select Committee on Intelligence, February 27, 1978.

Based on this review, it appears that no additional cost to the Governmnt would be incurred as a result of enactment of this bill.

Sincerely,

ALICE M. RIVLIN, *Director.*

CHANGES IN EXISTING LAW

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

UNITED STATES CODE

* * * * * * *

TITLE 18.—CRIMES AND CRIMINAL PROCEDURE

* * * * * * *

Chapter 119—WIRE INTERCEPTION OR INTERCEPTION OF ORAL COMMUNICATIONS

Sec.

2510. Definitions.
2511. Interception and disclosure of wire or oral communications prohibited.
2512. Manufacture, distribution, possession, and advertisement of wire or oral communication intercepting devices prohibited.
2513. Confiscation of wire or oral communication intercepting devices.
2515. Prohibition of use as evidence of intercepted wire or oral communications.
2516. Authorization for interception of wire or oral communications.
2517. Authorization for disclosure and use of intercepted wire or oral communications.
2518. Procedure for interception of wire or oral communications.
2519. Reports concerning intercepted wire or oral communications.
2520. Recovery of civil damages authorized.

§ 2510. Definitions

As used in this chapter—

(1) "wire communication" means any communication made in whole or in part through the use of facilities for the transmission

of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception 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;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device;

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire or oral communication other than—

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business; or (ii) being used by a communications common carrier in the ordinary course of its business, or by an investigation or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) "contents", which used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means—

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire or oral communications;

(10) "communication common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) of title 47 of the United States Code; and

(11) "aggrieved person" means a person who was a party to any intercepted wire or oral communication or a person against whom the interception was directed.

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

(1) Except as otherwise specifically provided in this chapter *or chapter 120 or with respect to techniques used by law enforcement officers not involving the interception of wire or oral communications as otherwise authorized by a search warrant or order of a court of competent jurisdiction*, any person who—

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

(b) willfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device, is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce, or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

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

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

(2) (a) (i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of any com-

munication common carrier, whose facilities are used in the transmission of a wire communication *or radio communication*, to intercept *or otherwise acquire*, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication: *Provided*, That said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

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

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

(2) in the case of an emergency interception or electronic surveillance as provided for in section 2518(7) of this chapter or section 2525(d) of chapter 120, a certification under oath by investigative or law enforcement officer that the applicable statutory requirements have been met,

any setting forth the period of time for which the electronic surveillance is authorized and describing the facilities from which the communication is to be acquired. Any violation of this subsection by a communication common carrier or an officer, employee, or agency thereof, shall render the carrier liable for the civil damages provided for in section 2520. No communication common carrier or officer, employee, or agent thereof shall disclose the existence of any interception under this chapter or electronic surveillance, as defined in chapter 120, with respect to which the common carrier has been furnished either an order or certification under this subparagraph, except as may otherwise be lawfully ordered."

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

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

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire or oral communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State or for the purpose of committing any other injurious act.

(e) Notwithstanding any other provision of this title or sections 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 under procedures approved by the Attorney General to conduct electronic surveillance as defined in section 2521(b)(6) of chapter 120 without a court order for the sole purpose of:

(i) testing the capability of electronic equipment, provided that no particular United States person shall be intentionally targeted for testing purposes without his consent, the test period shall be limited in event and duration to that necessary to determine the capability of the equipment, that the content of any communication acquired under this paragraph shall be retained and used only for the purpose of determiing the capability of such equipment, shall be disclosed only to the persons conducting the test, and shall be destroyed upon completion of the testing, and that the test may exceed ninety days only with the prior approval of the Attorney General; or

(ii) determining the existence and capability of electronic surveillance equipment being used unlawfully, provided that no particular United States person shall be intentionally targeted for such purposes without his consent, that such electronic surveillance shall be limited in extent and duration to that necessary to determine the existence and capability of such equipment, and that any information acquired by such surveillance shall be used only to enforce this chapter or section 605 of the Communications Act of 1934 or to protect information from unlawful surveillance.

(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 comunications by a means other than electronic surveillance as defined in section 2521(b)(6) of this title; and the procedures in this chapter and chapter 120 of this title, shall be the exclusive means by which electronic surveillance, as defined in section 2521(b)(6) of chapter 120, 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 in-

formation 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.]

* * * * * * *

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

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

* * * * * * *

§ 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.

* * * * * * *

§ 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.

* * * * * * *

§ 2520. Recovery of civil damages authorized

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

(a) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;

(b) punitive damages; and

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

A good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under this chapter or under any other law.

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

Sec.

2521. Definitions.
2522. Authorization for electronic surveillance of foreign intelligence purposes.
2523. Designation of judges authorized to grant orders for electronic surveillance.

Sec.
2524. Application for an order.
2525. Issuance of an order.
2526. Use of information.
2527. Report of electronic surveillance.
2528. Congressional oversight.

§ 2521. Definitions

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

(b) *As used in this chapter—*

(1) *"Foreign power" means—*

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

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

(C) *an entity, which is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;*

(D) *a foreign-based terrorist group;*

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

(F) *an entity which is directed and controlled by a foreign government or governments.*

(2) *"Agent of a foreign power" means—*

(A) *any person, other than a United States person, who—*

(i) *acts in the United States as an officer or employee of a foreign power; or*

(ii) *acts for or on behalf of a foreign power which engages in clandestine intelligence activities 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 conspires with any person knowing that such person is engaged in such activities;*

(B) *any person who—*

(i) *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;*

(ii) *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;*

(iii) *knowingly engages in sabotage or terrorism, or activities which are of may be in preparation therefor, for or on behalf of a foreign power;*

(iv) *knowingly aids or abets any person in the conduct of activities described in subparagraph (B)(i)–(iii) above, or conspires with any person knowing that*

such person is engaged in activities described in subparagraph (B)(i)–(iii) above: Provided, That no United States person may be considered an agent of a foreign power solely upon the basis of activities protected by the First Amendment to the Constitution of the United States.

(3) "Terrorism" means activities which—

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

(B) appear to be intended—

(i) to intimidate or coerce the civilian population,

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

(iii) to affect the conduct of a government by assassination or kidnapping.

(4) "Sabotage" means activities which would be prohibited by title 18, United States Code, chapter 105, if committed against the United States.

(5) "Foreign intelligence information" means—

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

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

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

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

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

(i) sabotage or terrorism by a foreign power or an agent of a foreign power, or

(ii) the clandestine intelligence activities of an intelligence service or network of a foreign power or an agent of a foreign power.

(6) "Electronic surveillance" means—

(A) the acquisition by an electronic, mechanical, or other surveillance device of the contents of 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, where 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;

(B) 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, where such acquisition occurs in the United States while the communication is being transmitted by wire;

(C) 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 where both the sender and all intended recipients are located within the United States; or

(D) 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.

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

(8) "Minimization procedures" means procedures which are reasonably designed to minimize the acquisition and retention, and prohibit the dissemination, except as provided for in subsections 2526 (a) and (b), of any information concerning United States persons without their consent that does not relate to the ability of the United States—

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

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

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

(D) to protect against terrorism by a foreign power or an agent of a foreign power;

(E) to protect against sabotage by a foreign power or an agent of a foreign power; or

(F) to protect against the clandestine intelligence activities of an intelligence service or network of a foreign power or an agent of a foreign power; and which are reasonably designed to insure that information which relates solely to the ability of the United States to provide for the national defense or security of the Nation and to provide for the conduct of the foreign affairs of the United States, under subparagraph (B) and (C) above, shall not be disseminated in a manner which identifies any United States person, without such person's consent, unless such person's identity is necessary to understand or assess the importance of information with respect to a foreign power or foreign territory or such information is otherwise publicly available.

(9) "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 not including corporations or associations which are foreign powers as defined in section 2521 (b) (1) (A)–(E).

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

§ 2522. Authorization for electronic surveillance for foreign intelligence purposes

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

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

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

(b) The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a special court of review which shall have jurisdiction to review the denial of any application made under this chapter. If such special court determines that the application was properly denied, the special court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

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

(d) Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, provided that the judges first designated under subsection (a) shall be designated for terms of from one to seven years so that one term expires each year, and that judges first designated under subsection (b) shall be designated for terms of three, five, and seven years.

§ 2524. Application for an order

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

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

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

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

(5) a statement of the proposed minimization procedures;

(6) when the target of the surveillance is not a foreign power as defined in section 2521(b)(1) (A), (B), or (C), a detailed description of the nature of the information sought;

(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) including a designation of the type of foreign intelligence information being sought according to the categories described in section 2521(b)(5);

(E) when the target of the surveillance is not a foreign power, as defined in section 2521(b)(1) (A), (B), or (C), 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;*

(F) *when the target of the surveillance is a foreign power, as defined in section 2521(b)(1) (A), (B), or (C), stating the period of time for which the surveillance is required to be maintained;*

(8) *when the target of the surveillance is not a foreign power, as defined in section 2521(b)(1) (A), (B), or (C), a statement of the means by which the surveillance will be effected, and when the target is a foreign power, as defined in section 2521(b)(1) (A), (B), or (C), a designation of the type of electronic surveillance to be used according to the categories described in section 2521 (b)(6) and a statement whether physical entry is required to effect the surveillance;*

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

(10) *when the target of the surveillance is not a foreign power, as defined in section 2521(b)(1) (A), (B), or (C), a statement of the period of time for which the electronic surveillance is required to be maintained. If the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this chapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter.*

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

(c) *The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 2525 of this chapter.*

§ 2525. *Issuance of an order*

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

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

(2) *the 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; and*

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

(4) *the proposed minimization procedures meet the definition of minimization procedures under section 2521(b)(8) of this title;*

(5) *the application which has been filed contains the descrip-*

tion and certification or certifications, specified in section 2524(a)(7) 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 2524(a)(7)(E) and any other information furnished under section 2524(c).

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

(1) specify—

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

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

(C) when the target of the surveillance is not a foreign power as defined in section 2521(b)(1)(A), (B), or (C), the type of information sought to be acquired and when the target is a foreign power defined in section 2521(b)(1)(A), (B), or (C), the designation of the type of foreign intelligence information under section 2521(b)(5) sought to be acquired;

(D) when the target of the surveillance is not a foreign power, as defined in section 2521(b)(1)(A), (B), or (C), the means by which the electronic surveillance will be effected, and when the target is a foreign power, as defined in section 2521(b)(1)(A), (B), or (C), a designation of the type of electronic surveillance to be used according to the categories described in section 2521(b)(6) and whether physical entry will be used to effect the surveillance;

(E) the period of time during which the electronic surveillance is approved; 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, contractor, 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, contractor, 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 which such person wishes to retain;

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

(c) An order issued under this section may approve an electronic surveillance not targeted against a foreign power, as defined in section 2521(b)(1)(A), (B), or (C), for the period necessary to achieve its purpose, or for ninety days, whichever is less; an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 2521(b)(1)(A), (B), or (C) for the

period specified in the certification required in section 2524(a)(7)(F), or for one year, whichever is less. Extensions of an order issued under this chapter may be granted on the same basis as an original order upon an application for an extension made in the same manner as required for an original application and after new findings required by subsection (a) of this section. In connection with applications for extensions where the target is not a foreign power, as defined in section 2521(b)(1)(A), (B), or (C), the judge may require the applicant to submit information, obtained pursuant to the original order or to any previous extensions, as may be necessary to make new findings of probable cause. 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 required by this chapter.

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

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

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

§ 2526. *Use of information*

(a) Information concerning United States persons acquired from an electronic surveillance conducted pursuant to this chapter may be used and disclosed by Federal officers and employees without the consent of the United States person only for purposes specified in section 2521(b)(8) (A) through (F), and in accordance with the minimization procedures required by this chapter, or for the enforcement of the criminal law if its use outweighs the possible harm to the national security. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character. No information acquired from an electronic surveillance conducted pursuant to this chapter may be used or disclosed by federal officers or employees except for lawful purposes.

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

(c) Whenever the Government of the United States, of a State, or of a 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, or other authority of the United States, a State, or a political subdivision thereof, any information obtained or derived from an electronic surveillance, 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 the information or submit it in evidence notify the court in which the information is to be disclosed or used or, if the information is to be disclosed or used in or before another authority, shall notify a court in the district wherein the information is to be so disclosed or so used that the Government intends to so disclose or so use such information.

(d) Any person who has been a subject of electronic surveillance and against whom evidence derived from such electronic surveillance is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or proceeding in or before any court, department officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any communication acquired by electronic surveillance, or evidence derived therefrom, on the grounds that—

(1) the communication was unlawfully acquired; or

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

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

(e) Whenever any court is notified in accordance with subsection (c), or whenever a motion is made by an aggrieved person pursuant to subsection (d), to suppress evidence on the grounds that it was obtained or derived from an unlawful electronic surveillance, or whenever any motion or request is made by an aggrieved person pursuant to section 3504 of this title or any other statute or rule of the United

States, to discover, obtain or suppress evidence or information obtained or derived from electronic surveillance, the federal court, or where the motion is made before another authority, a federal court in the same district as the authority, shall, notwithstanding any other law, if the Government by affidavit asserts that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and other materials relating to the surveillance as may be necessary to determine whether the surveillance was authorized and conducted in a manner that did not violate any right afforded by the Constitution and statutes of the United States to the aggrieved person. In making this determination, the court shall disclose to the aggrieved person portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance. If the court determines that the electronic surveillance of the aggrieved person was not lawfully authorized or conducted, the court shall in accordance with the requirements of law suppress the information obtained or evidence derived from the unlawful electronic surveillance. If the court determines that the surveillance was lawfully authorized and conducted, the court shall deny any motion for disclosure or discovery unless required by due process.

(f) If an emergency employment of the electronic surveillance is authorized under section 2525(d) and a subsequent order approving the suveillance 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.

(g) 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 where both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, except with the approval of the Attorney General where the contents indicate a threat of death or serious bodily harm to any person.

§ 2527. *Report of electronic surveillance*

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

(1) the total number of applications made for orders and extensions of orders approving electronic surveillance; and

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

§ 2528. *Congressional Oversight*

(a) 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 chapter. Nothing in this chapter shall be deemed to limit the authority and responsibility of those committees to obtain such additional information as they may need to carry out their respective functions and duties.

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

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

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

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

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

ADDITIONAL VIEWS OF SENATOR MALCOLM WALLOP

This bill fills an important need. Title III of the Omnibus Crime Act of 1968 did not regulate the executive branch's authority to conduct electronic surveillance for purposes of national security. In 1972 the Supreme Court's *Keith* decision brought electronic surveillance conducted for purposes of national security into the scope of the fourth amendment, and strongly suggested that Congress regulate such surveillance. Since that time, the executive agencies which normally carry out such surveillance have been under massive but conflicting political pressures to surveil and not to surveil. In the case of FBI Special Agent John Kearney, for example, we see a conflict between the need to catch the group which, among other things, bombed the Capitol on the one hand, and some interpretations of the crime bill of 1968 and the *Keith* decision on the other. We also see standards in this field evolving rapidly and perhaps being applied retroactively. The executive agencies have reacted as one might expect. Earlier this year the Attorney General told us that, with one exception, no American citizen was then the target of electronic surveillance. It would be comforting to think this means no American citizens are involved in activities which merit surveillance. Instead it seems that those who normally should be surveilling are afraid to act without firm legal mandate. Their position is entirely understandable. Without fixed standards we cannot expect them to stick their necks out in order to protect the country. This bill provides such standards in limited circumstances. Were there to be a choice between this bill and the current state of things I should certainly choose the bill. The bill does give firm legal basis for action to agencies too disheartened to act without it. More important, it represents a genuine attempt—perhaps the first attempt by Congress—to think through and to balance the citizen's competing claims to security from foreign powers, their agents and international terrorists, and to security from electronic surveillance by his own Government.

The bill's premises are altogether reasonable. The power to conduct electronic surveillance for the purpose of gaining foreign intelligence and foreign counterintelligence is ancillary to the President's constitutional power to command the Armed Forces and to direct the Nation's foreign affairs. In order to be lawful however, the power of electronic surveillance, like all other powers, must be exercised only for the purpose for which it was intended. Each exercise of power must be reasonably and proportionally related to the end for which the power exists. The bill therefore was written in order to allow the executive branch to conduct such electronic surveillance—but only such electronic surveillance—as is necessary to gather the intelligence and counterintelligence information truly needed by the country.

Hence the bill attempts to define the persons who may be surveilled, and the circumstances under which they may be surveilled, as well as the nature of the information to be sought. In addition the bill sets forth standards for the use to which information so gained may be put.

The bill presents the Congress with issues of two different kinds. One is the appropriateness of the definitions of persons, circumstances and information. I will argue below that these should be somewhat different than they are. The second, more important, has to do with the role which the bill assigns to the Judiciary.

The judiciary's role

In answer to concerns that the Judiciary is being made to rule on the substance of decisions affecting defense and foreign affairs, the argument has been made that the Judiciary's role in the bill is minimal. The burden of developing the case for surveillance is to rest on the executive branch. The executive branch will have to apply the bill's definitions. The judge, so goes the argument, will merely receive the certification and, when the persons to be surveilled are not U.S. persons will automatically allow the executive branch to proceed. The judge will not have to decide the merits of the cases, nor will he personally decide whether there is "probable cause" for looking at the case as the executive does. He will merely make sure that the executive branch has adhered to the standards set forth by the bill and its accompanying report in determining whether the person(s) in question may be surveilled. The judge will, however, have to control how the information is used. In the first instance the judge's role is merely a clerical one. It could be performed by OMB, by the GAO, or by the staff of any congressional committee. In the second instance the judge's task is managerial. In neither instance is it judicial. Why then confide it to judges? The answer seems to be that judges add an aura of legality to the process. The judicial branch however may not consent to provide rubber stamps and low-level managers for the executive branch. Thus where the judiciary's role is small it is both superfluous and, above all, nonjudicial.

Where U.S. persons are or may be concerned, however, the judiciary's role is undeniably larger. In such case the bill requires the judge to decide whether the executive branch's application of the criteria is or is not "clearly erroneous." Because this places the judge in the position of deciding on the propriety of the executive branch's decision, it raises a number of constitutional questions.

Heretofore the judicial branch has resisted temptations to declare itself competent in foreign affairs and defense. In the case of *Chicago Southern* v. *Waterman Steamship Co.* (333 U.S. 103, 111, 1948), the Supreme Court acknowledged the court's incompetence in matters of foreign intelligence. The substance of such matters, said the courts "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." Such decisions are in "the domain of political power, not subject to judicial intrusion or inquiry."

Clearly, defense and foreign relations are political tasks. That is to say, they are to be conducted subject to the people's power to elect.

The power to surveil for purposes of defense and foreign affairs belongs to that branch of government empowered by the Constitution to command the armed forces and conduct foreign affairs. There are no judicial criteria for interpreting whether this or that foreign visitor is or is not an agent of a foreign power, whether this or that American's connection with persons who may have some relation with the intelligence services of a foreign power has sufficient connections to warrant surveillance.

There are legitimate questions regarding the proper role of the Judiciary in society involved here. In the past we have seen legislation which has directed the courts to check the procedural regularity of the executive branch's actions. All too often we have seen the courts follow the valid logic that one cannot make judgments on procedure without reaching substance, and assume the authority for substantive review. The most recent instance is that of environmental law. Some judges are quite ready to move into foreign affairs in an equally substantive way. Judge Wright has written in the *Zweibon* case (516 F2nd 594 DC Circuit Court, 1975) that judges possess the "analytical ability or sensitivity of foreign affairs necessary to evaluate recommendations" for electronic surveillance. Furthermore, according to Judge Wright, "a Federal judge has lifetime tenure and could presumably develop an expertise in the field of foreign affairs if consistently presented to for authorizations for foreign security wiretaps." No doubt, a judge could; the large question is whether a judge should.

The above mentioned logic would operate swiftly in the areas covered by the bill. Is this information, a judge will have to decide, really necessary to protect the United States against grave hostile acts? Just how hostile is that country toward the United States? Will his information really contribute to the successful conduct of our relations with that country? And what, after all, is success with regard to that country? We must ask whether it would be wise, never mind constitutional, to place judgments on foreign affairs and defense into the hands of people who are not democratically responsible. Has the country so benefited from judicial activism in domestic affairs that it wishes to give judges responsibilities for foreign affairs and defense as well? And if, under the bill, one wished to minimize the amount of substantive judgment exercised by judges, how could he go about excluding from the special court people who think as Judge Wright does?

The judges would be put in an impossible position. They would have to become either the executive's rubber-stamps or the executive's competitors.

The role assigned to the judiciary by the bill also appears somewhat alien to the old Anglo-American tradition that the judicial power may deal only with concrete adversary situations. Unlike European judges, ours until very recently have not issued advisory opinions on administrative proceedings. The judgment of "not clearly erroneous" envisaged by the bill looks like an advisory opinion because the procedure for the warrant is entirely ex parte and because in nearly all cases the warrant procedure will be the entirety of the legal proceeding. The cases which would come before the special court would not, and would not be expected to, go beyond the procedure for

the warrant. Only incidentally some would result in real trials. But trials are precisely the concrete adversary proceedings which make judgments issued in ex parte proceedings something other than advisory opinions.

Ex parte proceedings which do not normally result in trials are also questionable from the standpoint of individual rights. Unless there is ultimately a trial, the individual affected will never have an opportunity to contest the government's case. Indeed, a body of case law is likely to grow without benefit of arguments contrary to the Government. If the judicial proceedings envisaged by the bill are to be final ones—that is, if they are not to end in trials—then there should at least be a kind of public defender or devil's advocate to argue against the executive branch's position. In the end we must decide whether these are to be real judicial proceedings or not.

The secrecy of the entire proceedings is itself quite foreign to our legal and constitutional system. Can our legal system stand a body of secret case law? It is not altogether clear that all the judges would be privy to the records of all the cases. If they were not, what good could dissenting opinions do? In the end, the only real means available to a dissenting judge or Justice of the Supreme Court, if he deemed a Government act of surveillance grossly abusive, would be to break secrecy and make the case public. It is far from clear that any action short of impeachment could be taken against such a judge. The bill, in short, raises the possibility of a constitutional clash.

In a sense the bill succeeds too well. Under it, each and every act of electronic surveillance authorized by the special court would be ipso facto legal. That is not an unmixed blessing, for it would curtail drastically Congress' ability to question the appropriateness of any such act. Under the bill, the intelligence committees of Congress may indeed have access to all information regarding requests for surveillance and their disposition. But what could any Congressman or Senator do about any act of surveillance he considered unjust or inappropriate? That act would have been not only requested under congressional standards, but certified as meeting those standards by a Federal judge. For all practical purposes the Congressman or Senator would face a res adjudicata. His chances of righting what he considered a wrong would be small—especially if he belonged to the minority party, and if the act of surveillance tended to favor the persons or policies of the majority party. Past abuses of the President's power of electronic surveillance for purposes of national security were not stopped by the judiciary, but by the only agency with the political power to do it: Congress. The judiciary's role in this bill would reduce Congress' latitude for action in this area.

The bill, however, gives the unfortunate appearance of trying to turn political questions into legal ones resolvable by judges not subject to election. It is doubtful whether this can be done in this case.

Is it possible under our Constitution for ordinary legislation to take away the President's power to do what he deems necessary to successfully command this country's defense forces and to successfully run our foreign relations? Let there be no mistake that the bill tries to do this when it stipulates that before exercising a power that is acknowledged to be his, he must receive authorization from a judge. The

principle that would be established here is that any given action of the executive which may affect the constitutional rights of citizens must be judicially deemed reasonable or "not clearly erroneous" before the fact. A moment's reflection is enough to conjure up any number of absurd situations which would be created by the application of this principle. None of this is to say that there can be no check upon the exercise of presidential powers, but rather to indicate that such checks should be political and must be after the fact.

The bill could achieve its worthy intended purpose, and yet avoid all the above mentioned difficulties if only two changes were made: (1) the review of the executive's certification that a particular act of electronic surveillance conforms to the bill's standards should occur after rather than before the fact, and (2) the reviewing body ought not to be a special court but two subcommittees of the intelligence committees of the Congress.

Standards

The shortcomings in the bill's standards proceed from three principal causes. First and foremost the bill confuses surveillance conducted for the purpose of gaining information necessary to the defense and foreign affairs of the United States with surveillance for the purpose of enforcing criminal law. Second, in several places the bill leaves to the judge the task of deciding questions on which its authors could not agree. Third, the standards are unduly complex.

The judge may not approve surveillance of U.S. persons unless the Government can show that he or she "knowingly engaged in clandestine intelligence activities which involve or may involve a violation of the criminal statutes of the United States" or knowingly commits, prepares to commit, or aids in the preparation or commission of, acts of sabotage or terrorism. In other words, in order to make himself eligible for surveillance someone not only has to have done something which could land him in jail, but he has to have done it knowingly. The latter, of course, is hard enough to show in a trial, never mind a hearing. Then there is the fact that most clandestine intelligence activities do not break the law, as shown by the recent case of the East German agent James Sattler. Such activities—secret communications and interviews with Government officials—may include violations of law. But who could blame a judge for deciding that an activity which does not violate the law does not in fact involve a violation of law? Indeed, the report states that activity protected by the Constitution of the United States may form no part of the basis for a finding that a person should be surveiled.

But even if these standards were made permissive enough to explicitly permit the surveillance of persons such as Mr. Sattler, or even of thoroughly innocent dupes, they would still divert the bill from its national purpose: surveillance of persons not for law enforcement but for the very sake of the information to be obtained. In cases where the defense or foreign relations of the United States are concerned, the subject's culpability or responsibility is arguably beside the point. The information gained by surveilling him may not relate to him at all, but may save countless lives. Consider the case of someone with knowledge of a band of nuclear terrorists, hiding in one of a thousand

apartments in a huge complex. It would be both reasonable and easy to tap every telephone in the complex, discard all intercepts but the correct one, and gain the vital information. But that would involve 999 violations of this bill. Consider also the cases of thoroughly innocent persons used as couriers by foreign agents. By surveilling them we could uncover other parts of a dangerous network. The bill does not allow us to. Consider, finally, the case of a thoroughly innocent American who may have knowledge which, unbeknownst to him, would shed light on foreign military or intelligence plans, and who would be placed in danger if contacted. Under this bill this American could not be surveilled. Whether or not to intrude upon the privacy of the abovementioned Americans would involve decisions of foreign and defense policy, not criminal law. The unwarranted confusion of the two serves neither well.

In some places the bill's standards—as elucidated in the report—are all too explicit. An example is the report's detailed discussion of why, under the standards of the bill, the surveillance of persons who worked to defeat the U.S. effort in Vietnam would be unlawful. The Judiciary Committee report states that during the Vietnam War some activists had coordinated their anti-U.S. efforts with North Vietnam and other Communist powers, but that since they operated autonomously rather than at the behest of Communist regimes, they would have been immune from surveillance under this bill. This kind of ex post facto exoneration of one side of a controversy and indictment of the other is, at best, gratuitous.

These descriptions set forth distinctions where I doubt the American people would find difference. For example, the report says:

> * * * direction from personnel of a foreign power which are not connected with an intelligence service or a network would not be a basis for electronic surveillance . . .

Leaving aside the enormous practical difficulty of probing for the connections between the several component parts of foreign powers, especially given the state of our intelligence, one cannot escape the question of how many "cutouts" are enough to exempt an American acting on behalf of or in conjunction with a Communist regime from lawful electronic surveillance? Most Americans would probably agree that in such cases it would be better to err on the side of caution and tell the intelligence agencies to survey anyone working with such regimes. The bill ought to reflect this.

Finally, the very complexity of the standards must be judged a drawback. Even if they provided the Nation sufficient protection in peacetime, they would surely be too cumbersome to do so in time of war. In time of war, then, a new bill would have to be hastily enacted to provide for emergency powers. But emergency legislation is generally bad legislation. While we have the time we ought to enact a bill workable in bad times as well as in good times.

MALCOLM WALLOP.