95TH CONGRESS } SENATE } REPT. 95–
1st Session } 604 Part 2

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1977

NOVEMBER 22 (legislative day, NOVEMBER 1), 1977.—Ordered to be printed

Mr. ABOUREZK (for Mr. KENNEDY), from the Committee on the Judiciary, submitted the following

REPORT

PART II—APPENDIX TO THE MINORITY VIEWS OF SENATOR JAMES ABOURZEK

[To accompany S. 1566]

The Committee on the Judiciary, 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.

EXPLANATORY NOTE

Due to an oversight, the appendix to the minority views of Senator James Abourezk, referred to in footnote 3 on page 83 of Senate Report 95–604, was not printed.

The appendix consists of six hypothetical cases, supplied by the Justice Department, to support the claimed need for a "noncriminal standard" in S. 1566, along with an analysis of each case done by the Washington office of the American Civil Liberties Union.

The appendix is as follows:

APPENDIX.—THE JUSTICE DEPARTMENT HYPOTHETICALS

In response to questions posed by Senator James Abourezk, Attorney General Griffin Bell sent a letter to the Senate Judiciary Committee wherein he outlined six hypothetical cases which Justice Department officials contend warrant a departure from a criminal standard in the Foreign Intelligence Surveillance Act of 1977. According to the Justice Department, these cases could not be reached under current espionage laws. After studying the cases, it is our contention that in three of the cases outlined, a judge would issue a warrant under current

espionage laws and that in the remaining three cases, a judge would not issue a warrant even under S. 1566 as currently drafted. In sum, the administration has not made a case for departing from the criminal standard in this act.

Case No. 1

"*A Spinelli-qualified*[1] informant reports that A has, pursuant to a foreign intelligence service's direction, collected and transmitted sensitive economic information concerning IBM trade secrets and advanced technological research which ultimately would have a variety of uses including possible use in a sophisticated weapons system, but which is not done pursuant to a Government contract. A is placed under physical surveillance and is seen to fill dead drops which are cleared by a member of a Communist Bloc embassy suspected of being an agent of its foreign intelligence service."

Comment.—This case turns on whether commercial information such as an IBM trade secret which might be used in a sophisticated weapons system constitutes "national defense" information or information "relating" to the national defense under 18 U.S.C. 794. The Justice Department contends that it may not. However, the Supreme Court, in *Gorin* v. *U.S.*, 312 U.S. 19 (1941), stated: "National defense . . . is a 'generic concept of broad connotations, referring to the military and naval establishments and the related activities of military and naval establishments and the related activities of national preparedness.' We agree that the words 'national defense' in the espionage act carry that meaning." *Id.* at 28. Thus, if a court found that a person fit all of the other criteria of 2521(b)(2)(B) and that the information being gathered was from an industrial source, it still would have no difficulty finding that there was probable cause to believe that 18 U.S.C. 794 was being violated.

Case No. 2

"Pursuant to the physical surveillance of a known foreign intelligence officer, B is seen to clear dead drops filled by that officer. On the second Tuesday of every month B drives by the officer's residence, after engaging in driving maneuvers intended to shake any surveillance. Within 1 block of the officer's residence B always sends a coded citizen's band radio transmission. B is discovered to have cultivated a close relationship with a State Department employee of the opposite sex specializing on matters dealing with the country of the intelligence agent."

Comment.—First it is not clear who the Government wants to place under electronic surveillance. Unless the vague "conspiracy" section, 2521(b)(2)(iii) remains in the bill, the State Department employee could not be wiretapped. Of course, the conspiracy section should be stricken from the bill. The Justice Department does believe it has probable cause to tap B under S. 1566. However, it would also have the authority to seek a warrant if 18 U.S.C. 794 were the standard.

The Justice Department seems to assume that it is necessary to know precisely what the content of the information is to establish

[1] *Spinelli* v. *United States*, 393 U.S. 410 (1969), states the requirements by which the reliability of an informant and his information must be tested for purposes of obtaining a search warrant.

what law is being violated, if any, in order to secure a warrant. However, the fact that the information is being passed to a "known foreign intelligence officer" should be sufficient to establish probable cause under 794. Moreover, 2521(b)(2)(B)(i) does not appear to require that the court find that a particular statute will be violated but only that the activities "involve or will involve a violation of the criminal statutes of the United States." And given the very broad interpretation of the phrase "national defense" by the Supreme Court, it is doubtful that any court would pause to inquire into the contents of the material before issuing a warrant. Certainly since all other elements required by S. 1566 have been met, a court would have probable cause to believe that a conspiracy to violate 18 U.S.C. 794 was underway.

Case No. 3

"C, using highly sophisticated equipment developed in a hostile foreign country, taps and data transmissions lines of several electronics corporations. These lines do not carry communications which can be aurally acquired, nor do they carry classified information, but the information carried, which is not available to the public, when put together, can give valuable information concerning components which are used in U.S. weapons systems."

Comment.—This case, like case No. 1, turns on the meaning of "national defense" and "related" information in current espionage laws. Nothing in section 793 of title 18 limits such information to data that is classified or developed pursuant to contract. Again, given the Court's broad reading in *Gorin*, the "valuable information concerning components which are used in U.S. weapons systems" would be covered under 18 U.S.C. 794. Since all the other element under 2521(b)(2)(B) have been met, there would be probable cause to find that a conspiracy to violate section 794 of title 18 existed.

Case No. 4

"D, a headwaiter in a fashionable Washington, D.C. restaurant, acts as a bookmaker and procurer for several well known and highly placed customers. A *Spinelli*-qualified informant reports that D has been instructed by a foreign intelligence service to relay all embarrassing and personally damaging information about these customers to a resident agent of the foreign intelligence service in Washington. The informant reports that at least one customer has been blackmailed in his job as a Government executive into taking positions favorable to the nation for which the resident agent works."

Comment.—No warrant could be issued either under section 794 of title 18 or under S. 1566. D is not collecting or transmitting information of the kind referred to by S. 1566 or section 794 of title 18. If the Justice Department's argument is that by getting one kind of information, D could trade it for another, then the Justice Department is interpreting S. 1566 in a way which eliminates the safeguards built into it. Moreover, one should also ask if it is necessary to tap this person. For example, his contact at the embassy could be tapped under the "foreign power" provision of S. 1566 and D could be surveilled by less intrusive means. Those who come into contact with D could be warned.

Case No. 5

"A *Spinelli*-qualified informant reports that E has, pursuant to the direction of a foreign intelligence service, engaged in various burglaries in the New York area of homes of U.S. employees of the United Nations to obtain information concerning U.S. positions in the United Nations."

Comment.—First of all, U.S. employees at the United Nations do not have advance information on U.S. positions at the United Nations. In any case, this situation is trivial. Such information should not be in an employee's home and E could be arrested for burglary. Or is the Justice Department assuming that E discusses his burglary targets on the phone?

Case No. 6

"A telephone tap of a foreign intelligence officer in the United States reveals that F, acting pursuant to the officer's direction, has infiltrated several refugee organizations in the United States. His instructions are to recruit members of these organizations under the guise that he is an agent of a refugee terrorist leader and then to target these recruited persons against the FBI, the Dade County Police, and the CIA, the ultimate goal being to infiltrate these agencies. F is to keep the intelligence officer informed as to his progress in this regard but his reports are to be made by mail, because the U.S. Government cannot open the mail unless a crime is being committed.

Comment.—As in case No. 4, no tap would be permitted under S. 1566. This is not the kind of information contemplated under the act. A tap would not be permitted under section 794 of title 18 as well. If F is to report in "by mail" is F going to do his recruitment by telephone? Does the Government plan to read S. 1566 to permit the refugee organizations to be wiretapped to find out if they are infiltrated? These are dangerous readings of S. 1566. The proper action is to allow the FBI, having this much information, to foil F's scheme.

In sum, the Justice Department is "reaching" for the exceptional case to establish the need for a deviation from the criminal standard. Contrary to all experience with judicial warrants in the wiretapping area, the Department presumes "strict construction" by judges will hamper legitimate intelligence. The Justice Department should be reminded that only seven judges, picked by the Chief Justice of the U.S. Supreme Court, will review these warrant requests. Of course, this does not give the Justice Department any certainty that all applications will be approved. But the criminal standard does not appreciably make the process more risky for the Government. On the other hand, the noncriminal standard is a dangerous precedent for abuse.

○

95TH CONGRESS } SENATE { REPORT
1st Session } { No. 95-604

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1977

NOVEMBER 15 (legislative day, NOVEMBER 1), 1977.—Ordered to be printed

Mr. KENNEDY, from the Committee on the Judiciary, submitted the following

REPORT

together with

MINORITY VIEWS

[To accompany S. 1566]

The Committee on the Judiciary, 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 3, line 17, strike out the word "knowingly".

On page 3, line 18, strike the word "a" and insert in lieu thereof the word "any"; and after the word "person" insert the words "knowing that such person is engaged in activities".

On page 4, line 20, strike out the word "knowingly".

On page 4, line 21, after the word "person" insert the words "knowing that such person is".

On page 4, line 22, strike the word "or" and insert in lieu thereof a dash, "—".

On page 8, strike lines 3 and 4 and insert in lieu thereof "or the Deputy Attorney General."

On page 8, line 7, insert the words "prohibit the" before the word "dissemination", and following the word "dissemination" insert ", except as provided for in subsections 2526 (a) and (b).".

On page 9, line 24, before the word "which", insert the words "or associations".

On page 14, line 21, strike the semicolon at the end of the line and insert in lieu thereof: "and a statement whether physical entry is required to effect the surveillance:".

29-010—77

On page 17, line 7, before the word "the" insert the following: "when the target of the surveillance is not a foreign power as defined in section 2521(b)(1)(A), (B), or (C),".

On page 17, line 8, strike the semicolon and insert in lieu thereof the following: "and when the target is a foreign power as 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;".

On page 17, line 16, strike the semicolon and insert in lieu thereof the following: "and whether physical entry will be used to effect the surveillance;".

On page 21, line 11, insert the following sentence after the period: "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.".

On page 21, line 22, after the word "States,", insert the following: "a State, or a political subdivision thereof.".

On page 22, line 7, after the word "information.", strike the remainder of the subsection through line 6 on page 23 and insert in lieu thereof the following new subsections:

"(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 or approval.

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

"(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 nationl 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."

On page 23, line 7, renumber subsection "(b)" as "(f)".

On page 26, line 16, insert the word, "the" before the word, "investigative."

On page 29, insert after line 13 a new subsection as follows:

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

On page 29, line 14, strike "(i)" and substitute in lieu thereof "(j)".

On page 29, line 17, strike "(j)" and substitute in lieu thereof, "(k)".

On page 30, line 2, following the words "provided that" insert "no particular United States person shall be intentionally targeted for testing purposes without his consent."

Purpose of Amendments

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

Finally, the reported bill adds an amendment 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). This latter amendment is technical and conforming in nature and is 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 for the authorization of applications for a court order approving the use of electronic surveillance 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.

S. 1566 has its origin in S. 3197, "The Foreign Intelligence Surveillance Act of 1976", 94th Cong. 2d Sess. (1976). That legislation, also introduced by Senator Kennedy with broad, bipartisan support, including that of the Ford Administration, 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 to 2 nays, but the Session ended before the full Senate could act on the legislation.

S. 1566 picks up where S. 3197 left off. Following the introduction of the measure, two days of hearings were held by the Subcommittee on Criminal Laws and Procedures, chaired by Senator Kennedy at the request of Senator McClellan. Eight witnesses testified, and a number of other individuals submitted statements for the hearing record. Among those testifying were Attorney General Griffin B. Bell; Director of the FBI, Clarence Kelley; Director of the Central Intelligence Agency, Stansfield Turner; Secretary of Defense Harold Brown; John Shattuck of the American Civil Liberties Union; and Morton H. Halperin of the Center for National Security Studies.

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

S. 1566 as reported, however, has been amended in relative minor respects to respond to the constructive criticisms and suggestions elicited in the hearings. As amended, the bill was approved by the Subcommittee on Criminal Laws and Procedures with a unanimous recommendation for favorable action.

Position of the Administration

The Administration supports the enactment of S. 1566 and has supported its swift passage. 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 positive 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

The bill reported by the Judiciary Committee amends title 18, United States Code, by adding a new chapter after chapter 119, en-

[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. (Statement of Attorney General Griffin B. Bell).

titled "Electronic Surveillance Within the United States for Foreign Intelligence Purposes." The purpose of the bill is to provide a procedure under which the Attorney General can obtain a judicial warrant authorizing the use of electronic surveillance in the United States for foreign intelligence purposes. If enacted, this legislation would require a judicial warrant authorizing the following for foreign intelligence purposes:

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

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

(c) The acquisition of a private radio transmission in which all of the communicants are located within the United States; or

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

S. 1566 authorizes the Chief Justice of the United States to designate seven district court judges, any one of whom may hear applications for and grant orders approving electronic surveillance for foreign intelligence purposes. The bill further provides that the Chief Justice shall designate three judges from the United States district courts or courts of appeals to sit as a special Court of Appeals to hear appeals by the United States from denials of applications made by any one of the seven district court judges. The United States may further appeal from this special court to the Supreme Court.

Under S. 1566, a judge may issue a warrant authorizing electronic surveillance within the United States only if he finds that: the President has authorized the Attorney General to approve applications for such electronic surveillance; the application has been approved by the Attorney General; on the basis of the facts submitted to the court, there is probable cause to believe that the target of the surveillance is a foreign power or an agent of a foreign power; the place at which the surveillance is directed is being used or about to be used by that foreign power or agent; minimization procedures to be followed are reasonably designed to minimize the acquisition and retention of information relating to Americans that is not foreign intelligence information; Executive certification that the information sought is foreign intelligence information which cannot reasonably be obtained by normal investigative techniques; and, if the target of the surveillance is a United States person, such certification is not clearly erroneous. The order may approve the electronic surveillance for no longer than 90 days with respect to all natural persons and some foreign powers, but extensions of up to 90 days may be granted upon an application and after the same findings as required for the original order. With respect to official "foreign powers", as defined in the legislation, the approval may be for as long as one year.

In the event that an emergency arises and resort to a court is not possible, the Attorney General is authorized to approve electronic

surveillance. Such an emergency surveillance cannot continue for more than 24 hours without a judge's approval; a judge must be immediately notified of the emergency surveillance; and an application must be made to the judge within 24 hours of approval of that emergency surveillance.

The bill would limit the use of information concerning United States citizens and lawful resident aliens acquired from electronic surveillances to matters properly related to foreign intelligence and the enforcement of criminal law. No information obtained from an electronic surveillance could be used or disclosed against any person except for lawful purposes. A judge may order the notification of a person under electronic surveillance if an emergency surveillance was authorized but subsequently disapproved by a judge.

S. 1566 provides for annual reports by the Attorney General to the Congress and the Administrative Office of the United States Courts containing statistical information relating to surveillances during the preceding year.

The bill does not provide statutory authorization for the use of any technique other than electronic surveillance, and, combined with chapter 119 of title 18, it constitutes the exclusive means by which electronic surveillance, as defined, and the interception of domestic wire and oral communications may be conducted; the bill recognizes no inherent power of the President in this area.

In three major respects S. 1566 increases the protections for United States citizens and lawful resident aliens over those contained in S. 3197. First, the definition of electronic surveillance has been expanded to include the targeting of United States persons in their international communications. This is specifically aimed at eliminating one of the abuses identified by the Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities and largely implements one of that Committee's recommendations. (Book II, Intelligence Activities and the Rights of Americans, S. Rept. 94–755, 94th Cong., 2d Sess. 309 (1976).) Second, when a United States citizen or lawful resident alien is the target of an electronic surveillance, the judge is required to review the Executive Branch certification to determine if it is clearly erroneous. No review of the certification was allowed in S. 3197. Finally, S. 1566 spells out that the Executive cannot engage in electronic surveillance within the United States without a prior judicial warrant. This is accomplished by repealing the so-called executive "inherent power" disclaimer clause currently found in section 2511(3) of Title 18, United States Code. S. 1566 provides instead that its statutory procedures (and those found in chapter 119 of title 18) "shall be the exclusive means" for conducting electronic surveillance, as defined in the legislation, in the United States. The highly controversial disclaimer has often been cited as evidence of a congressional ratification of the President's inherent constitutional power to engage in electronic surveillance in order to obtain foreign intelligence information essential to the national security. Despite the admonition of the Supreme Court that the language of the disclaimer was "neutral" and did not reflect any such congressional recognition of inherent power, the section has been a major source of controversy. By repeal-

ing section 2511(3) and expressly stating that the statutory warrant procedures spelled out in the law must be followed in conducting electronic surveillance in the United States, this legislation ends the eight-year debate over the meaning and scope of the inherent power disclaimer clause.

II. STATEMENT OF NEED

The Federal Government has never enacted legislation to regulate the use of electronic surveillance within the United States for foreign intelligence purposes. Although efforts have been made in recent years by Senator Kennedy, Senator Nelson, Senator Mathias, and former Senator Philip A. Hart to circumscribe the power of the executive branch to engage in such surveillance, and the Senate came very close to enacting such legislation during the 94th Congress, the fact remains that such efforts have never been successful.[2] The hearings held this year on S. 1566 were the sixth set of hearings on warrantless wiretapping in as many years.[3] The Committee believes that S. 1566 is a measure which can successfully break this impasse and provide effective, reasonable safeguards to ensure accountability and prevent improper surveillance. S. 1566 goes a long way in striking a fair and just balance between protection of national security and protection of personal liberties. It is a recognition by both the Executive Branch and the Congress that the statutory rule of law must prevail in the area of foreign intelligence surveillance.

The need for such statutory safeguards has become apparent in recent years. This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused. These abuses were initially illuminated in 1973 during the investigation of the Watergate break-in. Since that time, however, the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, chaired by Senator Church (hereafter referred to as the Church Committee), has concluded that every President since Franklin D. Roosevelt asserted the authority to authorize warrantless electronic surveillance and exercised that authority. While the number of illegal or improper national security taps and bugs conducted during the Nixon administration may have exceeded those in previous administrations, the surveillances were regrettably by no means atypical. In summarizing its

---

[2] See, e.g., S. 3197, *Foreign Intelligence Surveillance Act of 1976*, 94th Cong., 2d sess. (1976); S. 743, *National Security Surveillance Act of 1975*, 94th Cong., 1st sess. (1975); S. 2820, *Surveillance Practices and Procedures Act of 1973*, 93rd Cong., 1st sess. (1973); S. 4062, *Freedom from Surveillance Act of 1974*, 93rd Cong., 2d sess. (1974).

[3] See, e.g., Hearings before the Subcommittee on Criminal Laws and Procedures of the Senate Committee on the Judiciary, *Foreign Intelligence Surveillance Act of 1976*, 94th Cong., 2d sess. (1976); Senate Select Committee on Intelligence, *Foreign Intelligence Surveillance Act of 1976*, 94th Cong., 2d sess. (1976); Subcommittee on Surveillance of the Senate Committee on Foreign Relations and the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, *Warrantless Wiretaping and Electronic Surveillance*, 94th Cong., 1st sess. (1975); Joint Hearings before the Subcommittee on Administrative Practice and Procedure and the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, *Warrantless Wiretapping and Electronic Surveillance*, 93d Cong., 2d sess. (1974); Hearings before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, *Warrantless Wiretapping*, 92d Cong., 2d sess. (1972). In the joint report of the Subcommittees on Surveillance and Administrative Practice and Procedure issued in 1975, findings were made that "there are not adequate written standards or criteria within the executive branch to govern the warrantless electronic surveillance of either Americans or foreigners. There is a gap in the statutes, the case, and in administrative regulation on the use of warrantless wiretaps or bugs by executive branch agencies for alleged 'national security' purposes."

conclusion that surveillance was "often conducted by illegal or improper means," the Church committee wrote:

> Since the 1930's, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of judicial warrant. . . . [P]ast subjects of these surveillances have included a United States Congressman, Congressional staff member, journalists and newsmen, and numerous individuals and groups who engaged in no criminal activity and who posed no genuine threat to the national security, such as two White House domestic affairs advisers and an anti-Vietnam War protest group. (vol. 2, p. 12)

* * * * *

> The application of vague and elastic standards for wiretapping and bugging has resulted in electronic surveillances which, by any objective measure, were improper and seriously infringed the Fourth Amendment Rights of both the targets and those with whom the targets communicated. The inherently intrusive nature of electronic surveillance, moreover, has enabled the Government to generate vast amounts of information—unrelated to any legitimate government interest—about the personal and political lives of American citizens. The collection of this type of information has, in turn, raised the danger of its use for partisan political and other improper ends by senior administration officials. (vol. 3, p. 32.)

Also formidable—although incalculable—is the "chilling effect" which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of the surveillance, but who perceived themselves, whether reasonably or unreasonably, as potential targets. Our Bill of Rights is concerned not only with direct infringements on constitutional rights, but also with government activities which effectively inhibit the exercise of these rights. The exercise of political freedom depends in large measure on citizens' understanding that they will be able to be publicly active and dissent from official policy, within lawful limits, without having to sacrifice the expectation of privacy that they rightfully hold. Arbitrary or uncontrolled use of warrantless electronic surveillance can violate that understanding and impair that public confidence so necessary to an uninhibited political life.

S. 1566 is designed, therefore, to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it. At the same time, however, this legislation does not prohibit the legitimate use of electronic surveillance to obtain foreign intelligence information. As the Church committee pointed out:

> Electronic surveillance techniques have understandably enabled these agencies to obtain valuable information relevant to their legitimate intelligence missions. Use of these techniques has provided the Government with vital intelligence, which would be difficult to acquire through other means, about the activities and intentions of foreign powers and has

provided important leads in counterespionage cases. (vol. 2, p. 274)

Safeguarding national security against the intelligence activities of foreign agents remains a vitally important Government purpose. Few would dispute the fact that we live in a dangerous world in which hostile intelligence activities in this country are still carried on to our detriment.

Striking a sound balance between the need for such surveillance and the protection of civil liberties lies at the heart of S. 1566. As Senator Kennedy stated in introducing S. 1566:

> The complexity of the problem must not be underestimated. Electronic surveillance can be a useful tool for the Government's gathering of certain kinds of information; yet, if abused, it can also constitute a particularly indiscriminate and penetrating invasion of the privacy of our citizens. My objective over the past six years has been to reach some kind of fair balance that will protect the security of the United States without infringing on our citizens' human liberties and rights.[4]

The committee believes that the Executive Branch of Government should have, under proper circumstances and with appropriate safeguards, authority to acquire important foreign intelligence information by means of electronic surveillance. The committee also believes that the past record and the state of the law in the area make it desirable that the Executive Branch not be the sole or final arbiter of when such proper circumstances exist. S. 1566 is designed to permit the Government to gather necessary foreign intelligence information by means of electronic surveillance but under limitations and according to procedural guidelines which will better safeguard the rights of individuals.

III. BACKGROUND

The bipartisan congressional support for S. 1566 and the constructive cooperation of the Executive Branch toward the legislation signifies a constructive change in the ongoing debate over electronic surveillance. That debate has centered around the power of the President to acquire information necessary for the national security and the constitutionality of warrantless electronic surveillance. This is not surprising since the United States Supreme Court has never expressly decided the issue of whether the President has constitutional authority to authorize warrantless electronic surveillance in cases concerning foreign intelligence. Whether the President has so-called "inherent power" to engage in or authorize warrantless electronic surveillance and, if such power exists, what limitations, if any, restrict the scope of that power, are issues which have troubled constitutional scholars for decades.

The history of warrantless electronic surveillance offers support to both proponents and critics of the concept of "inherent power" and clearly highlights the need for passage of S. 1566.

In 1928, the Supreme Court in *Olmstead* v. *United States* [5] held that wiretapping was not within the coverage of the Fourth Amendment.

[4] 123 Cong. Rec. S7857 (daily ed., May 18, 1977).
[5] 277 U.S. 468.

Three years later, Attorney General William D. Mitchell authorized telephone wiretapping, upon the personal approval of bureau chiefs, of syndicated bootleggers and in "exceptional cases where the crimes are substantial and serious, and the necessity is great and [the bureau chief and the Assistant Attorney General] are satisfied that the persons whose wires are to be tapped are of the criminal type." These general guidelines governed the Department's practice through the thirties and telephone wiretapping was considered to be an important law enforcement tool.[6]

Congress placed the first restrictions on wiretapping in the Federal Communications Act of 1934, which made it a crime for any person "to intercept and divulge or publish the contents of wire and radio communications." [7] The Supreme Court construed this section to apply to Federal agents and held that evidence obtained from the interception of wire and radio communications, and the fruits of that evidence, were inadmissible in court.[8] However, the Justice Department did not interpret the Federal Communications Act or the *Nardone* decision as prohibiting the interception of wire communications *per se*; rather only the interception and divulgence of their contents outside the Federal establishment was considered to be unlawful. Thus, the Justice Department found continued authority for its national security wiretaps.

In 1940, President Roosevelt issued a memorandum to the Attorney General stating his view that electronic surveillance would be proper under the Constitution where "grave matters involving defense of the nation" were involved. The President authorized and directed the Attorney General "to secure information by listening devices [directed at] the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies." The Attorney General was requested "to limit these investigations so conducted to a minimum and to limit them insofar as possible as to aliens." [9]

This practice was continued in successive administrations. In 1946, Attorney General Tom C. Clark sent President Truman a letter informing him of President Roosevelt's directive. Clark's memorandum, however, omitted the portion of President Roosevelt's directive limiting wiretaps "insofar as posible to aliens." Instead, he recommended that the directive "be continued in force" in view of the "increase in subversive activities" and "a very substantial increase in crime." President Truman approved.[10]

---

[6] The history of the practice of the Department of Justice which follows in this Report is derived from Attorney General Edward H. Levi's testimony before the Church committee on Novmber 6, 1975 and the final report of that committee. The relevant portions of the report include Book I, *Foreign and Military Intelligence,* chapter IX, "Counterintelligence:" Book II, *Intelligence Activities and the Rights of Americans,* chapter II, "The Growth of Domestic Intelligence," finding C, "Excessive Use of Intrusive Techniques," and finding E, "Political Abuse of Intelligence Information"; Book III, *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans,* "Dr. Martin Luther King, Jr., Case Study," "Warrantless FBI Electronic Surveillance," Warrantless Surreptitious Entries," "Domestic CIA and FBI Mail Opening," National Security Agency Surveillance Affecting Americans," and "National Security, Civil Liberties, and the Collection of Intelligence: A Report on the Huston Plan"; Book IV, *Supplementary Detailed Staff Reports on Foreign and Military Intelligence,* "Intelligence and Technology."

[7] 47 U.S.C. 605 (1964 ed.), 48 Stat. 1103.

[8] *Nardone* v. *United States,* 302 U.S. 379 (1937); 308 U.S. 338 (1939).

[9] III Church committee 297.

[10] II Church committee 60. In 1950, aides to President Truman discovered Clark's incomplete quotation, and the President considered returning to the terms of the original 1940 authorization. However, the 1946 directive was never rescinded.

In the early fifties, however, Attorney General J. Howard McGrath took the position that he would not approve or authorize the installation of microphone surveillances by means of trespass. This policy was quickly reversed by Attorney General Herbert Brownell in 1954 in a sweeping memorandum to FBI Director Hoover instructing him that the Bureau was indeed authorized to conduct such trespassory surveillances regardless of the fact of surreptitious entry, and without the need to first acquire the Attorney General's authorization. Such surveillance was simply authorized whenever the Bureau concluded that the "national interest" so required. The Brownell memorandum is instructive:

> It is my opinion that the department should adopt that interpretation which will permit microphone coverage by the FBI in a manner most conducive to our national interest. I recognize that for the FBI to fulfill its important intelligence function, considerations of internal security and the national interest are paramount; and, therefore, may compel the unrestricted use of this technique in the national interest.[11]

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

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

> [I]n the internal security field, we are utilizing microphone surveillances on a restricted basis even though trespass is necessary to assist in uncovering the activities of Soviet intelligence agents and Communist party leaders. In the interests of national safety, microphone surveillances are also utilized on a restricted basis, even though trespass is necessary, in uncovering major criminal activities. We are using such coverage in connection with our investigations of the clandestine activities of top hoodlums and organized crime. From an intelligence standpoint, this investigative technique has produced results unobtainable through other means. The information so obtained is treated in the same manner as information obtained from wiretaps, that is, not from the standpoint of evidentiary value but for intelligence purposes.[12]

The policy of the Department of Justice was stated publicly in 1966 by the Solicitor General in a supplemental brief to the Supreme Court in *Black* v. *United States*.[13] Referring to the general delegation of authority by Attorneys General to the Director of the Bureau, the Solicitor stated:

> An exception to the general delegation of authority has been prescribed, since 1940, for the interception of wire com-

[11] III Church committee 297.
[12] III Church committee 297.
[13] 385 U.S. 26 (1966).

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

In *Katz* v. *United States*, 389 U.S. 347 (1967), the Supreme Court finally discarded the *Olmstead* doctrine and held that the Fourth Amendment's warrant provision did apply to electronic surveillance. The Court explicitly declined, however, to extend its holding to cases "involving the national security." 389 U.S. at 358, n. 23. The next year, Congress followed suit: responding to the *Katz* case, Congress enacted the Omnibus Crime Control and Safe Streets Act (18 U.S.C. sections 2510–2520).[14] Title III of that Act established a procedure for the judicial authorization of electronic surveillance for the investigation and prevention of specified types of serious crimes and the use of the product of such surveillance in court proceedings. It prohibited wiretapping and electronic surveillance by persons other than duly authorized law enforcement officers, personnel of the Federal Communications Commission, or communication common carriers monitoring communications in the normal course of their employment.

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

> Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation

[14] See also, S. Rept. 1097, *Senate Committee on the Judiciary, Omnibus Crime Control and Safe Streets Act of 1967*; 90th Cong., 2d sess. (1968).

against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other clear and present danger to the structure or existence of the Government.

Against this background the Supreme Court decided the *Keith* [15] case in 1972. While the issue was narrowly drawn—"the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval" (407 U.S. at 301)—the court's opinion inevitably shed some light on the deeper problem of balancing conflicting interests in national security cases (407 U.S., at 320–321) :

1. The Court took notice of the long-standing Justice Department policy of warrantless electronic surveillance. It also recognized the "elementary truth" that "unless Government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered." [16]

2. In balancing the constitutional rights involved against the governmental objectives, the Court noted the "convergence of First and Fourth amendment values not ordinarily present in cases of "ordinary" crime." [17] The Court went on to pose the issue: "If the legitimate need of the Government to safeguard domestic security requires the use of electronic surveillance the question is whether the needs of citizens for privacy and free expression may not be better protected by requiring a warrant before such surveillance is undertaken. We must also ask whether a warrant requirement would unduly frustrate the efforts of Government to protect itself from acts of subversion and overthrow directed against it." [18]

3. In concluding that a warrant was required in domestic security surveillance cases, the Court emphasized the traditional reasons for requiring a warrant: [19]

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

[15] *United States* v. *United States District Court,* 407 U.S. 297 (1972).
[16] 407 U.S., at 312.
[17] 407 U.S., at 313.
[18] 407 U.S., at 315.
[19] 407 U.S., at 316–317.

4. The Court then went on to consider and reject the Government's argument that the disclosure of information in a warrant application posed the serious danger of leaks and the Government's argument that "internal security matters are too subtle and compex for judicial evaluation." [20] The Court observed that "[c]ourts regularly deal with the most difficult issues of our society. There is no reason to believe that Federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases." [21] As to the secrecy claim, the Court observed the "[t]he investigation of criminal activity has long involved imparting sensitive information to judicial officers who have respected the confidentialities involved." [22]

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

However, the Court emphasized that "this case involves only the domestic aspects of national security. We have not addressed, and expressed no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents." [23]

And, in construing the effect of the title III presidential disclaimer the court wrote: [24]

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

Since the *Keith* case, three circuit courts of appeals have addressed the question the Supreme Court reserved. The Fifth Circuit in *United States* v. *Brown*, 484 F.2d 418 (5th Cir. 1973), cert. denied, 415 U.S. 960 (1974), upheld the legality of a surveillance in which the defendant, an American citizen, was incidentally overheard as a result of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes. The court found that on the basis of "the President's constitutional duty to act for the United States in the field of foreign affairs, and his inherent power to protect national security in the conduct of foreign affairs . . . the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence." [25]

In *United States* v. *Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc), cert. denied *sub nom. Ivanov* v. *United States*, 419 U.S. 881 (1974), the Third Circuit similarly held that electronic surveillance conducted

[20] 407 U.S., at 320.
[21] 407 U.S., at 320.
[22] 407 U.S., at 320–321.
[23] 407 U.S., at 321–322.
[24] 407 U.S., at 303, 306.
[25] 484 F. 2d at 426.

without a warrant would be lawful so long as the primary purpose was to obtain foreign intelligence information. The court found that such surveillance would be reasonable under the Fourth Amendment without a warrant even though it might involve the overhearing of conversations.

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

Although the holding of *Zweibon* was limited to the case of a domestic organization without ties to a foreign power, the plurality opinion of the court—in legal analysis closely patterned on *Keith*—concluded "that an analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional." [26]

Thus, after almost 50 years of case law dealing with the subject of warrantless electronic surveillance, and despite the practice of warrantless foreign intelligence surveillance sanctioned and engaged in by nine administrations, constitutional limits on the President's powers to order such surveillances remains an open question. This legislation would provide the secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights.

IV. Conclusion

S. 1566 would alter the current debate arising out of the uncertainty of the present law by completing an exclusive charter for the conduct of electronic surveillance in the United States. It would relegate to the past the wire-tapping abuses brought to light during the committee hearings by providing, for the first time, effective substantive and procedural statutory controls over foreign intelligence electronic surveillance.[27]

---

[26] 516 F.2d at 613–614. Neither *Brown* nor *Butenko* provide a systematic analysis of the problem within the framework indicated by the Supreme Court decision in *Keith*, i.e., whether the requirement of a warrant would unduly frustrate the exercise of the President's responsibility in the area of national security. The court's opinion in *Brown* simply confirmed the President's inherent power to authorize foreign intelligence collection through, among other things, electronic surveillance without a warrant. The *Butenko* opinion offers a sightly more extensive analysis of the problem. On the other hand, the *Zweibon* opinion, insofar as it considered and rejected the arguments for the existence of an inherent power by applying the analytical framework used by the Supreme Court in *Keith*, was a plurality opinion.

[27] The Church committee concluded that, in many cases, surveillance was based on the belief that groups or individuals were directed, financed or otherwise controlled by a hostile foreign power. Some of the surveillances were directed against citizens or organizations whose activities, while not necessarily violent, were thought to be sufficiently subversive to pose a danger to the security of the country. (III, pp. 316–317.) However, from this "subversive activities" standard it was, according to the committee, relatively easy to justify and order electronic surveillance against American citizens and organizations, not primarily because of their own activities, but because they were believed to be adversely influenced, whether consciously or not, by persons acting under the direction of foreign power. The electronic surveillance of Martin Luther King was justified not because King himself posed any threat to national security, but because of the possibility that two of King's advisers were associated with the Communist party. (III, p. 318.)

The infinite elasticity of the "national security" criteria unrestrained by any judicial or external check, has been dramatically underscored in recent years by a series of surveillances directed against Government employees and journalists for the avowed purposes of identifying the sources of "leaks" of classified information. (III, p. 321.)

The basis for this legislation is the understanding—concurred in by the Attorney General—that even if the President has an "inherent" constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing foreign intelligence surveillance.[28]

The bill provides external and internal checks on the executive. The external check is found in the judicial warrant procedure which requires the executive branch to secure a warrant before engaging in electronic surveillance for purposes of obtaining foreign intelligence information. Such surveillance would be limited to a "foreign power" and "agent of a foreign power." United States citizens and lawful resident aliens could be targets of electronic surveillance only if they are: (1) knowingly engaged in "clandestine intelligence activities which involve or will involve a violation" of the criminal law; (2) knowingly engaged in activities "that involve or will involve sabotage or terrorism for or on behalf of a foreign power"; or (3) "pursuant to the direction of an intelligence service or intelligence network of a foreign power" are knowingly or secretly collecting or transmitting foreign intelligence in a manner harmful to the security of the United States. All other persons—such as illegal aliens or foreign visitors—could also be targets if they are: (1) either officers or employees of a foreign power; or (2) are "knowingly engaging in clandestine intelligence activities for or on behalf of a foreign power under circumstances which indicate that such activities would be harmful to the security of the United States." For such surveillance to be undertaken, a judicial warrant must be secured on the basis of a showing of "probable cause" that the target is a "foreign power" or an "agent of a foreign power." Thus the courts for the first time will ultimately rule on whether such foreign intelligence surveillance should occur.

Before a warrant can be requested, a designated Executive Branch official must first certify in writing to the court that the information sought to be obtained is "foreign intelligence information" as defined, and that the purpose of the surveillance is to obtain such information. Moreover the Attorney General is required to make a finding that the requirements for a warrant application have been met before he authorizes the application. These provisions provide an internal check on applications for electronic surveillance by establishing a method of written accountability within the Executive Branch.

Other procedural safeguards assure that the Government will not engage in illegitimate eavesdropping or misuse of information so acquired. The bill requires that each order include a detailed procedure to minimize the extraneous or irrelevant information that might otherwise be obtained; information acquired concerning United States citizens or lawful resident aliens can be used and disclosed only for foreign intelligence purposes or in connection with the enforcement of the criminal law; even if the target is not a United States citizen or lawful resident alien information acquired can only be used for "lawful purposes"; detailed provisions safeguard the right of the criminal defendant to challenge the validity and propriety of the sur-

[28] Cf. *See Youngstown Sheet & Tube Co.* v. *Sawyer*, 343 U.S. 579 (1952) (Jackson, J. concurring).

veillance; if the target is an individual or specified types of foreign powers the application for a warrant must state the means by which the surveillance will be effected; when the target is an "official" foreign power, as defined, the application must still designate the type of electronic surveillance to be used and whether or not physical entry will be used to effect the surveillance; finally, the Attorney General is required to transmit to the Congress annually certain statistics concerning the surveillances engaged in during the preceding year.

Most importantly, the disclaimer in 18 U.S.C. § 2511(3) is replaced by provisions that assure that this bill, together with chapter 119, will be the *exclusive* means by which electronic surveillance covered by this bill, and the interception of wire and oral communications, may be conducted.

A difficult issue posed during committee deliberations was whether foreign intelligence electronic surveillance should be limited to situations involving the commission of a crime. S. 1566 provides four limited situations in which natural persons may be made the target of an electronic surveillance without a probable cause showing of criminal activity. The first and least problematic involves persons who are neither citizens nor permanent resident aliens but who are officers or employees of a "foreign power". This provision is primarily designed to cover foreigners who are employed in diplomatic and consular offices in the United States. It is unchanged from the provisions in S. 3197.

The second situation, which constitutes a major change from S. 3197, involves an alien (other than an alien who has been admitted for permanent resident) who "knowingly engages in clandestine intelligence activities for or on behalf of a foreign power under circumstances which indicate that such activities would be harmful to the security of the United States." S. 3197 made no such distinction between aliens and United States citizens in the application of the noncriminal standard. S. 1566, however, broadens the noncriminal standard of S. 3197 in cases involving nonresident aliens.

The third situation involves a United States citizen or permanent resident alien who, "pursuant to the direction of an intelligence service or intelligence network of a foreign power, knowingly collects or transmits information or material to an intelligence service or intelligence network of a foreign power in a manner intended to conceal the nature of such information or material or the fact of such transmission or collection, under circumstances which indicate the transmission of such information or material would be harmful to the security of the United States, or that lack of knowledge by the United States of such collection or transmission would be harmful to the security of the United States." This standard was also present in S. 3197 except for the addition of "collection" to the activities which would justify surveillance.

The last situation, and the one most disturbing to some members of the committee, is the change from S. 3197 allowing electronic surveillance of one who conspires with or aids or abets another engaged in the noncriminal activities described in the second and third situations. While the Committee feels this is justified, it should be emphasized that the aider or abetter cannot be an unknowing dupe. The bill re-

quires that he know that the person he is aiding is engaged in the described activities.

S. 3197 did not extend the doctrine of conspiracy to the non-criminal standard. Thus, insofar as S. 1566 loosens the language of the non-criminal standard for certain aliens, and permits the application of conspiracy to that standard in all cases, the bill posed problems to some members of the committee.

Although there is precedent for departing from a strict criminal standard in the issuance of search warrants deemed compatible with the fourth amendment, *see e.g.*, *Camara* v. *Municipal Court*, 387 U.S. 523 (1967); *Almeida-Sanchez* v. *United States*, 413 U.S. 266 (1973); *cf. United States* v. *Martinez-Fuerte*, 428 U.S. 543 (1976), (no warrant required at all), those decisions did not involve national security surveillance. It should also be pointed out, however, that in the *Keith* case, *supra*, the Supreme Court noted that the reasons for domestic security surveillance may differ from those justifying surveillance for domestic crimes and that, accordingly, "different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate needs of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizens rights deserving protection." [28] As indicated in the section-by-section analysis, this departure from the general principle that such surveillance must be linked to criminal activity is intended to be a narrow, circumscribed one, reflecting the deep concern of the committee. This bill authorizes electronic surveillance in a limited number of non-criminal situations only under the twin safeguards of an independent review by a neutral judge and his application of a "probable cause standard".

It is important to note that the committee's favorable recommendation of this legislation in no way reflects any judgment that it would also be appropriate to depart from the standard of criminal activity as the basis for using other intrusive investigative techniques. The bill does not impliedly authorize departure from the standard of criminality in other aspects of national security investigations or intelligence collection directed at Americans without the safeguards of judicial review and probable cause. It remains to determine, in fashioning a charter for the use of informants, physical surveillance and other investigative procedures, whether the departure from a criminal standard is an acceptable basis for investigating United States citizens on grounds of national security.

Conforming amendments in S. 1566 integrate existing electronic surveillance provisions in title III of the Omnibus Crime Control and Safe Streets Act with the new provisions of the bill.

Section-by-Section Analysis

Section 1 of the bill provides that the Act may be cited as the "Foreign Intelligence Surveillance Act of 1977".

Section 2 of the bill amends title 18, United States Code, by adding a new chapter 120 composed of sections 2521–2527 as follows:

[28] 407 U.S. at 322; see also, *Zweibon* v. *Mitchell*, 516 F. 2d at 669.

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 governmental establishments which 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 government which is substantially composed of permanent resident aliens or citizens of the United States.

(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 is a category which was not specifically delineated in S. 3197. Certain changes have been made in the S. 3197 warrant requirements with respect to specific foreign powers which generally require less information to be given to the judge and allow the surveillance to be continued for a longer period of time without the need for reauthorization. This decision to treat certain "foreign powers" differently in terms of warrant requirements was made at the insistence of the Administration. The Committee is satisfied, however, that the distinction is sufficiently limited so as not to pose any threat of abuse. Thus, it is only with respect to "entities" openly acknowledged by a foreign government to be directed and controlled by such foreign government—those which are clearly arms of a government or governments and not privately controlled—that are subject to the extended warrants granted on a lesser showing. Such "official" entities are treated in the same manner as the government they serve.

(4) "A foreign-based terrorist group." This category refers to a foreign-based group whose activities involve "terrorism", as defined. The committee recognizes that many international terrorist groups have members from various nations, and may not in fact have any clearly definable "base." Nevertheless, under this definition the group must be "foreign-based;" that is, it must not be based in the United States, although it may carry out terrorist acts in this country. It is the Committee's belief that a domestic terrorist group should be subjected to electronic surveillance only pursuant to Title III. Where, however, a group is not domestically based, but derives strength and refuge by organizing, planning, and preparing its terrorist activities outside the jurisdiction of the United States, then that group is a legitimate target for intelligence surveillance under this bill no matter what the citizenship of its members.

(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, those foreign political parties which are mere instrumentalities of a foreign government and which 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, found verbatim in S. 3197, would include an entity which appears to be a legitimate commercial establishment but which is actually being utilized by a foreign government as a cover for espionage activities. A law firm, public relations firm, or other legitimate concern which merely represents a foreign government or its interests is not, by definition, an entity under this category. The question of whether a group, commercial enterprise, or organization comes within the scope of this definition is one for the court to determine on the basis of a probable cause standard.

B. "Agent of a Foreign Power"

Subsection (b)(2) defines an "agent of a foreign power" in two separate ways. Subparagraph (A)(i) includes officers or employees of foreign powers who are not United States citizens or aliens lawfully admitted for permanent residence. The definition is framed in this way because it is presumed that nonresident aliens who are officers or employees of a foreign power are likely sources of foreign intelligence information. Given the tenuous relationship of foreign officers or employees with the United States and their close relationship with a foreign power, this standard is considered by the Committee to be reasonable in light of the Government's legitimate need for foreign intelligence information and the nature of the interests upon which the search would intrude. The reference to employees of a foreign power is meant to include those persons who have a normal employee-employer relationship.[18] The subparagraph is not intended to encompass such foreign visitors as professors, lecturers, exchange students, performers, or athletes, even if they are receiving remuneration or expenses from their home government in such capacity.

Subparagraphs (A)(ii), (iii) and (B) 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 engaged for or on behalf of a foreign power.

Subparagraph (A)(ii) defines an agent of a foreign power as a person who is not a citizen or resident alien of the United States who "knowingly engages in clandestine intelligence activities for or on behalf of a foreign power under circumstances which indicate that

[18] This bill is not intended, of course, to repeal or abrogate the Vienna Convention on Diplomatic Relations, which was ratified by the Senate and came into effect in the United States on December 13, 1972. The Convention provides that diplomatic agents, their residences (article 30(1)), and their missions (article 22 (1) and (3)), as well as their official correspondence (Article 27(2) and 30(2)), are "inviolable." The obligations of the Convention are reciprocal; when another nation has failed to maintain the inviolability of American diplomatic communications, this country is free under international law to act similarly towards representatives of that nation (article 47(2a)). The bill does not affect nor does the Committee intend to affect, the legal interpretations of the Vienna Convention under which the Executive Branch has made those treaty obligations effective within the United States.

such activities would be harmful to the United States." This category could potentially include illegal aliens, foreign terrorists, exchange visitors, foreign businessmen, foreign students, and foreign seamen. While it is expected that in most cases such foreigners would, even under this standard, be violating United States criminal laws, and would certainly be subject to deportation (see, e.g., 8 U.S.C. § 1251(a)(7)), there is no specific requirement that the activity providing the justification for the surveillance constitute a Federal crime. This separate non-criminal standard for foreigners is a significant change from S. 3197. In favorably reporting S. 3197 during the 94th Congress, the Committee accepted the need for a narrower noncriminal standard applicable to *all* persons within the United States. S. 1566, however, while retaining the S. 3197 noncriminal standard largely intact for United States citizens and lawful resident aliens, alters it substantially when other persons—not United States citizens or resident aliens—are the targets of the surveillance.

For example, no reference is made to the requirement of "direction" from a foreign power's "intelligence service or intelligence network", nor is there any requirement of "collection" or "transmission" in a secret manner. Because it eliminates such requirements when foreign visitors—and only when foreign visitors—are involved, the bill has been criticized by some members of the Committee. The Fourth Amendment to the Constitution speaks in terms of protecting all "persons"—not just United States citizens and law resident aliens—yet the bill establishes a different standard for illegal aliens and foreign visitors.

Proponents of the change, however, point out that where there are compelling considerations of national security, alienage distinctions are clearly lawful.[29] The Director of the FBI testified in support of the different standard. He pointed out that large numbers of temporary aliens visit the United States and that many of these aliens are working for foreign intelligence networks. The Select Committee on Intelligence Activities similarly identified the problem, pointing out that one quarter of the Soviet exchange students coming to the United States in a ten-year period were found to be intelligence officers.[30] This Committee is aware *that less intrusive investigative techniques may not be able to obtain sufficient information about persons visiting here only for a limited time:* the additional showing required for United States citizens and permanent resident aliens, therefore, may simply not be possible. Weighing these findings, recommendations, and considerations, as well as the recognized, bipartisan goal of enacting statutory safeguards in this area, the Committee has concluded that this distinction between United States citizens, lawful resident aliens and other aliens should be permitted.

It is clear, however, that this standard—unlike that in subparagraph (A)(i)—is not one which allows surveillance on the basis of the alien's status *per se*. The alien must be engaged in "clandestine intelligence activities" for or on behalf of a foreign power, and while these clandestine activities need not involve criminal violations (as they must for United States citizens and permanent resident aliens), they must be occurring under circumstances which indicate that the activi-

[29] See, e.g., *Hampton* v. *Mow Sun Wong*, 426 U.S. 88, 115 (1976).
[30] Book I, at 163–164.

ties would be harmful to the security of the United States. Additionally, of course, the determination that sufficient justification exists to conduct electronic surveillance of a foreign visitor or a nonresident alien will be made by a judge, and not a member of the Executive Branch.

Subparagraph (B) (i) is unchanged from the comparable provision S. 3197 and allows surveillance of any person, including a United States citizen or permanent resident alien, who is knowingly engaged in clandestine intelligence activities for or on behalf of a foreign power, which activities involve or will involve a violation of the criminal statutes of the United States. Under this standard the person to be surveilled must be shown to have a knowing and substantial connection with the foreign power for whom he is working. There must be a principal-agent relationship under which the alleged agent has undertaken to provide services for his foreign principal. The agent must also be knowingly engaged in "clandestine intelligence activities" which involve or will involve violations of federal criminal law. It is anticipated that most of the persons surveilled under this section will be violating the criminal espionage laws (Title 18, U.S. Code, sections 792–799, 951; title 42, U.S. Code, section 2272–2278b; and title 50, U.S. Code, section 855).

C. "Clandestine Intelligence Activities"

The term "clandestine intelligence activities" as used in the bill is directed primarily toward those traditional activities associated with "spying," that is gathering information in a clandestine manner or conducting covert operations for a foreign power.

In addition to those activities which fall within the substantive statutory crimes of spying are activities directly related to spying which are criminal within the meaning of the conspiracy, attempt, and aiding and abetting statutes. Examples would include maintaining a "safehouse" for secret meetings, servicing "letter drops" or "dead 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.

In addition to conventional "spying," that is, the gathering of information, the intelligence agencies of foreign powers also engage in covert action designed to influence events in this country. Under subparagraph (b) (i), if such political action is covert, involves a violation of federal criminal law, such as the bribery of a public official, and is undertaken directly on behalf of a foreign power, it would be encompassed by this subparagraph. The bill does not authorize electronic surveillance when the activities, even though not public and conducted for a foreign power, involve *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 trigger 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 involves 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, or form any part of the basis, for finding that any individual is engaged in "clandestine intelligence activities." As a corollary, even the lawful gathering of information done in a confidential manner which is a 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 activity" under this section, where such information gathering is a normal ancillary part of lobbying, organizing political protest, and other political activity protected by the first amendment. Clandestine collection of information regarding the business plans or trade secrets of an American company which merely might provide a competitive advantage to foreign firms, for example, in bidding on a contract with a third country would also not be "clandestine intelligence activity" under subsection (b) (i) unless the foreign disclosure of such financial or business information involved or would involve a violation of federal criminal law. Classified information held by private firms is covered in this way.

And, in the case of an organization whose leaders are engaged in clandestine intelligence activity, 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, or is conspiring with or knowingly aiding and abetting those who are, before electronic surveillance directed against him may be authorized under this chapter.

Whatever the nature of the activity in question, there must be a clandestine aspect. The statute requires that the alleged foreign agent not only be working for or on behalf of a foreign power or its agent, but also, as a separate requirement, that he be engaged in *clandestine* intelligence activity.

There must also be an effort to obtain information which is being kept secret and is not 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 contained in books, magazines, scientific journals, or newspapers would never constitute "clandestine intelligence activity." [31]

Finally, the word "involve" as used in subparagraph (b) (i) is not intended to encompass any individuals who are not actually engaged in a violation of federal law. It is intended to encompass a violation of federal law which is an integral part of the clandestine intelligence activity even though the clandestine intelligence activity itself

[31] It should be noted that even failing to comply fully with the Foreign Agents Registration Act (22 U.S.C. 611, et seq.) in and of itself is not intended to be clandestine intelligence activity merely because the agent seeks to lobby Congress or influence public opinion on matters relating to the national defense or foreign affairs. 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 is 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) (1) of S. 1566 if all the other statutory criteria were met.

might fall between the cracks of the espionage laws. For instance, foreign intelligence agents might be collecting sensitive industrial or technological information. While this collection may not violate the espionage laws, the agents may have to transport the material across state lines, thereby violating federal laws which proscribe the interstate transportation of stolen property. The phrase "will involve", which also appears in this subparagraph, is likewise in no way intended to diminish or dilute the nature of the criminal activity to be established. Its only purpose is to permit electronic surveillance at some point prior to the time when the actual crime sought to be prevented, for example the actual passage of classified documents, actually occurs. The Committee recognizes that 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 immediacy of the phrase "will 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 will be involved in clandestine intelligence activities.

Subparagraph (B)(ii) includes any person who knowingly engages in activities that involve or will involve sabotage or terrorism for or on behalf of a foreign power. The terms "sabotage" and "terrorism" are defined and require a showing of criminal activity. Again, the nature of the knowledge and agency relationship are the same as required under subparagraph (B)(i). In no event may mere sympathy for, identity of interest with, or vocal support for the goals of a foreign group, even a foreign terrorist group, be sufficient. The terms "involve" and "will involve" are intended to encompass activities directly supportive of some act of terrorism, *e.g.*, the purchase or surreptitious importation into the United States of explosives for use in a terrorist incident, or the planning for an assassination.

D. The Noncriminal Standard

Subparagraph (B)(iii) is the so-called non-criminal standard applicable to United States citizens and resident aliens. The only substantive change from the similar provision in S. 3197 is the inclusion—at the Administration's request—of "collection" among the activities justifying the surveillance. This change makes sense. Actual transmission of information to a foreign intelligence service may not yet be completed or may not be detected, yet, given the other criteria under this subparagraph, collection alone should be sufficient to justify the surveillance.

During the course of the hearings on S. 1566, testimony was elicited from various witnesses as to the precise contours of the noncriminal standard. All witnesses agreed that the phrase would, with limited exception for certain activity, refer to activity constituting a Federal or State crime. On the basis of testimony of, and discussions with, the

Department of Justice, the committee agreed to include language covering certain narrowly circumscribed intelligence activities closely related to criminal espionage but not presently constituting an offense under Federal law. Such a decision was made despite serious reservations voiced by various members of the Committee. In introducing S. 1566, Senator Kennedy stated that he had "never been altogether satisfied with the explanations offered by the Department of Justice as to why a noncriminal standard is necessary at all." [32] This view continues to be shared by many Committee members. However, for various reasons—perhaps the most important being the desire of the Committee to at long last enact important statutory safeguards in this area and to avoid the acrimony of past fruitless efforts—the Committee has again agreed to include in S. 1566 a narrow, carefully circumscribed, noncriminal standard. *The Administration has agreed, however, to draft a revision of the espionage laws which might enable this narrow noncriminal standard to be repealed.*[33] In the interim, the Committee believes that this subparagraph contains standards sufficiently stringent as to be incapable of abuse.

Although the Administration is committed to using the criminal standards wherever possible, there are several situations where this subparagraph may be necessary. For example, the situation where the information being collected or transmitted is not "information relating to the national defense," as defined by the courts. *Gorin* v. *United States*, 312 U.S. 19 (1941); *United States* v. *Heine*, 151 F.2d 813 (2d Cir. 1945) (L. Hand, J.), cert. denied, 328 U.S. 833 (1946). The example is also cited where Federal agents have witnessed a series of "meets" or "drops" between a hostile foreign intelligence officer and a citizen, information is being passed, but the federal agents have been unable to determine precisely what information is being transmitted. A third example referred to is where personally damaging information is being gathered about persons for purposes of blackmailing them into becoming foreign agents. This may or may not be a crime, depending on whether the technical requirements of the blackmail or extortion statutes have been satisfied, but the national security could be threatened, and electronic surveillance may enable the government to protect the victim from such attempts. Another example is where a foreign intelligence service is targeting the installations or personnel of a foreign government in the United States. There still must be a nexus to our national security, but such nexus may well exist where the foreign government is an ally of the United States and a compromise of the former's secrets to an adversary nation may endanger our own security.[34]

Because of this range of cases, which may or may not fall within the ambit of the espionage laws, but do involve Americans working for a foreign intelligence service under circumstances dangerous to the national security, the Committee has chosen to include this limited noncriminal standard for Americans. The bill permits, in this subpara-

[32] 123 Cong. Rec. S7857 (daily ed., May 18, 1977).
[33] *Senate Judiciary Hearings*, testimony of Attorney General Griffin Bell, pp 12-46 (June 13, 1977).
[34] Of course, nothing in this subparagraph would allow electronic surveillance of those engaged in protests, demonstrations, or other such lawful activity directed against a third country, even if carried out at the direction of a foreign power.

graph, the surveillance of any person if the Government can establish that there is probable cause to believe that:

(1) Said person was acting pursuant to the direction of a foreign intelligence service;

(2) Said person was knowingly either collecting or transmitting information or material to a foreign intelligence service in a manner intended to conceal either the nature of the information or material or the fact that it was being collected or transmitted; and

(3) The circumstances indicate that the transmission of the information or material would harm the security of the United States, or that lack of knowledge by the United States government about what is being transmitted would harm the security of the United States.

E. "Pursuant to the Direction of an Intelligence Service or Intelligence Network of a Foreign Power"

Perhaps the most important phrase in the subparagraph is the requirement that the target of the surveillance be acting "pursuant to the direction of an intelligence service or intelligence network of a foreign power." This language means that a person must be acting under the direction and control of such power.

There must be a principal-agency relationship under which the alleged agent has undertaken to do the bidding of his foreign principal. This subparagraph, therefore, would not authorize electronic surveillance of United States citizens or permanent resident aliens, whatever the nature of their alleged activities, unless there was probable cause to believe they are acting pursuant to the direction of a foreign intelligence service or network. It does not authorize electronic surveillance under any circumstances for the class of individuals included by the Supreme Court within the scope of the *Keith* decision requiring judicial warrants for alleged threats to security of a domestic nature. 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.

For example, Americans of Greek, Jewish, Irish, or Chinese extraction legitimately may seek to influence United States 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 intelligence service or network of a foreign power". Thus, such "direction" from personnel of a foreign power which 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 additional 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. The key legal doctrine is that of agency; 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 United States 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 had been 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 maximize worldwide public attention, that would not have sufficed 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 two 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 was engaged in the secret collection or transmission of information or material to a foreign power. 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 particular member was acting pursuant to the direction of a foreign intelligence service for purposes of this subparagraph.

Finally, it is necessary that the person be *aware* he is acting on behalf of a foreign power. An American might be secretly collecting information about important technology, for example, and have been misled into the belief he was acting for a research institute or a multinational corporation. Therefore it would not suffice to establish probable cause that the American is, *in fact*, 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's intelligence activities.

It also follows, of course, that evidence a foreign power is trying to recruit an American as an agent does not suffice to establish probable cause to believe he has agreed to do the foreign power's bidding and is engaged on its behalf. Before electronic surveillance could be directed

against the American, the court would have to find probable cause that the American had responded positively to the recruitment effort and it is now acting as a member of that power's intelligence network.

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

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

The Committee emphasizes that this narrow inclusion for electronic surveillance without probable cause to believe that the targets are engaged in criminal activity is, of course, not intended to provide a bootstrap for even broader authority to investigate noncriminal activity of Americans absent the safeguards in this bill. The Committee emphasizes that S. 1566 establishes a legislative scheme to deal only with electronic surveillance; the use of other investigative techniques do not fall within the scope of this bill.

F. "Conspires or Aids and Abets"

Subparagraphs (A)(iii) and (B)(iv) are provisions which allow electronic surveillance of persons who knowingly conspire with or aid or abet persons who could otherwise be subjected to electronic surveillance under the provisions discussed above. Insofar as the doctrines of conspiracy and aiding and abetting have been made applicable to the noncriminal standards of S. 1566—a change from S. 3197—some members of the Committee are concerned. They feel that the safeguards and protections found in the narrow, carefully circumscribed language of the noncriminal standards (especially in the noncriminal standard applicable to United States citizens) can be abused through the use of the conspiracy and aiding and abetting language.

Under (A)(iii) non-resident aliens can be subjected to electronic surveillance by conspiring with or aiding or abetting another nonresident alien, knowing that person is engaged in clandestine intelligence activities for or on behalf of a foreign power. Under (B)(iv) a person can be subjected to electronic surveillance if he conspires with or aids or abets a person knowing that person is engaged in the activities described in subparagraphs (B)(i) through (iii). Under

both (A)(iii) and (B)(iv) the Government would have to establish probable cause that the prospective target knew both that the person with whom he was conspiring or whom he was aiding or abetting was engaging in the described activities as an agent of a foreign power and that his own conduct was assisting or furthering such activity. The knowledge requirement is therefore applicable to both the status of the person being aided by the proposed subject of the surveillance and the nature of the activity being promoted. The innocent dupe who unwittingly aids a foreign intelligence officer cannot be targeted under this provision.[35]

An illustration of the "knowing" requirement is provided by the case of Dr. Martin Luther King. Dr. King was subjected to electronic surveillance on "national security grounds" when he continued to associate with two advisers whom the Government had apprised him were suspected of being American Communist party members and, by implication, agents of a foreign power. Dr. King's mere continued association and consultation with those advisers, despite the Government's warnings, would clearly not have been a sufficient basis under this bill to target Dr. King as the subject of electronic surveillance.

Indeed, even if there had been probable cause to believe that the advisers alleged to be Communists were engaged in criminal clandestine intelligence activity for a foreign power within the meaning of this section, and even if there were probable cause to believe Dr. King was aware they were acting for a foreign power, it would also have been necessary under this bill to establish probable cause that Dr. King was knowingly engaged in furthering his advisers' criminal clandestine intelligence activities. Absent one or more of these required showings, King could not have been found to be one who knowingly aids or abets a foreign agent.[36]

Subsection (b)(3) defines "terrorism" as criminal activities which are violent or dangerous to human life. The purpose of the activities must be either the forceful intimidation of the civilian population, the intimidation of national leaders in order to force a significant change in governmental policy, or the affecting of Governmental conduct by assassination or kidnaping. 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 foreign

[35] 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 their lawful activity.

[36] Mere membership in the United States Communist Party is not sufficient under this bill to establish probable cause that a person is acting under the direction and control of a foreign power or that he is engaged in clandestine intelligence activities.

Moreover, even if additional information established probable cause to believe some members of the party were acting under the direction and control 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 neither be criminal espionage nor the kind of economic or technical information relating to the national security whose collection might satisfy the noncriminal standard. Similarly, since the civil rights protest movement itself involved constitutionally protected rights of association, speech and petition for redress of grievances, efforts by a foreign power to involve itself in such a movement are intended to be specifically excluded from the definition of clandestine intelligence activity.

country, or the deliberate assassination of persons to strike fear into others to deter them from exercising their rights.

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 United States 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.[37] 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 was related to foreign intelligence as defined. The Committee agrees with the Administration that 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 before there is probable cause to believe that they will engage in sabotage against Federal facilities.

G. "Foreign Intelligence Information"

Subsection (b) (5) defines "foreign intelligence information" to include five types of information, which, while not mutually exclusive, tend to be distinguishable. Subparagraph (A) of this subsection is defined as information deemed necessary for the United States to protect itself against actual or potential attack or other similarly grave hostile acts of foreign power or its agents. This category is intended to encompass information which relates to foreign military capabilities and intentions, as well as acts of force or aggression which would have serious adverse consequences to the national security of the United States. The term "hostile acts" must be read in the context of the subparagraph which is keyed to actual or potential attack on the United States. Thus, only the most "grave" types of "hostile acts" would be envisioned as falling within this provision.[38]

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

---

[37] 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 and owned by a foreign government.

[38] In testifying last year in 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." (House Hearings 10–11, emphasis added.)

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).

Subparagraph (C) of this subsection includes information which is deemed necessary for the United States to protect against 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)(ii).

Subparagraph (D) of this subsection includes information which is deemed necessary for the United States to protect against sabotage by a foreign power or foreign agent.

Subparagraph (E) of this subsection includes information which is deemed 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 activities of clandestine intelligence services of foreign powers in the United States. This subsection is not intended to encompass information sought about dissident political activity by United States 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 past improper investigations of citizens and is not intended to be included as a permissible avenue of "foreign intelligence" collection under this subparagraph. Nor does this subparagraph include efforts to prevent "news leaks" or to prevent publication of such leaked information in the American press, unless there is reason to believe that such publication is itself being done by an agent of a foreign intelligence service and that such publication would harm the national security.

Most importantly, all five subparagraphs set out standards establishing a nexus between the information sought and the desired end. Subparagraph (B) requires that the information sought be "essential" while the other subparagraphs establish a standard of "necessary."

Where the term "necessary" is used, the Committee intends to require more than a showing that the information would be useful or convenient. When the term "essential" is used, the Committee intends to require a showing that the information is important and required but not that it is of utmost importance or indispensable.

The use of these standards is intended by the committee to mandate that a significant degree of need be demonstrated by those seeking the surveillance. For example, it is often contended that the 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.

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

In addition, information about a United States citizen's private affairs shall not be deemed "foreign intelligence information" unless it directly relates to his activities on behalf of a foreign power. This interest 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 deemed necessary or essentional. For example, the government could not seek purely personal information about a United States citizen or permanent resident alien, who is a suspected spy, upon a theory that it might learn something which would be "compromising." Instead, the bill makes clear that the only information about United States citizens or permanent resident aliens which may be sought must not only be necessary to the ability of the U.S. to protect against clandestine intelligence activities, but must also "relate to" the activities themselves. This restriction might not always be fully applicable to agents of foreign powers as defined in Section 2521(b)(2)(A)(i), 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.

H. "Electronic Surveillance"

Paragraph (6) defines "electronic surveillance" to include four separate types of activities.

Subparagraph (A) makes a major improvement over the language of S. 3197 by protecting United States citizens and resident aliens in the United States from being targeted in their international communications without a judicial warrant no matter where the surveillance is being carried out. Under S. 3197 such targeting did not fall within the confines of the bill; this provision is, therefore, a significant extension of the protections afforded United States citizens and lawful resident aliens. The subparagraph specifically brings within the procedures of S. 1566 the acquisition of the contents of a wire or radio communication of United States citizens and permanent resident aliens in the United States by intentionally targeting that particular, known United States citizen or resident alien, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. Thus, for example, the "watch-listing" activities of the National Security Agency, if directed against United States citizens in the United States, would require a warrant under this regulation.

Subparagraph (B) includes the acquisition, by an electronic, mechanical, or other surveillance device, of the contents of a wire communication without the consent of any party thereto when such acquisition occurs in the United States while the communication is being transmitted by wire. As this subdefinition makes clear, the location of the parties to the wire communication is immaterial if the acquisition occurs within the United States. Thus, either a wholly domestic telephone call or an international telephone call can be the subject of electronic surveillance under this subdefinition if the acquisition of the content of the call takes place in this country and if such acquisition occurs "while the communication is being transmitted by wire." This second qualifier is necessary because the definition of "wire communicatoin" 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 United States citizen or resident alien in the United States.

Subparagraph (C) includes the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of a radio communication, without the consent of any party thereto, made with a reasonable expectation of privacy 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, *i.e.*, a totally domestic radio communication. This part of the definition would reach not only the acquisition of communications made wholly by radio but also the acquisition of "wire communications" by means of intercepting the radio transmitted portion of those communications 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 communicants. Thus, the acquisition of radio communications outside the territorial limits of the United States would be covered if all of the communicants were located within the United States. Only acquisition of those domestic radio communications made with a reasonable expectation of privacy 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* v. *Hall*, 488 F.2d 193 (9th Cir. 1973).

Only "intentional" acquisitions of domestic 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 accidently and unintentionally acquire communications intended to be totally domestic. It is the Committee's under-

standing that these communications are immediately destroyed. Absent the word "intentional", however, these accidental interceptions, even if the contents are immediately destroyed, could leave these agencies open to civil or criminal liability for failing to secure a judicial warrant.

The effect of subparagraphs (A), (B) and (C) of Section 2521 (b)(6), therefore, is to include within the term "electronic surveillance" 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 18 U.S.C. Section 2510(1), except those international wire communications which are acquired by intercepting the radio transmitted portions of the communications, and the targeting of particular United States citizens or resident aliens in the United States in order to acquire international communications made with a reasonable expectation of privacy.

The reason for excepting from the definition of "electronic surveillance" the acquisition of international radio transmissions, including international wire communications when acquired by intercepting radio transmissions when not accomplished by targeting a particular United States person in the United States, is to exempt from the procedures of the bill certain signals intelligence activities of the National Security Agency.

Although it is desirable to develop legislative controls in this area, the Committee has concluded that these practices are sufficiently different from traditional electronic surveillance techniques, both conceptually and technologically, that, except when they target particular United States citizens or resident aliens in the United States, they should be considered separately by the Congress.[39] The fact that this bill does not bring these activities within its purview, however, should not be viewed as congressional authorization of such activities. This committee merely recognizes that this particular signals intelligence activity is not covered by the procedures outlined in this bill. In any case, the requirements of the Fourth Amendment would, of course, continue to apply to this type of communications intelligence activity.[40]

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 cir-

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

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

cumstances 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 oversight. 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 United States 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.[41] But two persons in a public park, far from any stranger, would not reasonably anticipate that their conversations could be overhead from afar through a directional microphone, and so would retain their right of privacy. Of course, law enforcement officials may, if they wish, continue to obtain an ordinary search warrant or chapter 119 court order if the facts and circumstances so justify it.

The definition of "electronic surveillance" comprising the interception of wire communications and radio transmissions has an explicit exception where any party has consented to the interception. This is intended to 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.[42] Whether consent may be inferred in a particular case will depend on the facts and circumstances.

That part of the definition of "electronic surveillance" regarding the installation of a device requires that the acquisition of information be under circumstances in which a person has a constitutionally protected right of privacy. There is no such right in those situations where the interception is consented to by at least one party to the conversation. For instance, a body microphone placed on an informer with his consent is an installation of a device to acquire information, but a person speaking to the informer has no justifiable expectation that the informer will not repeat, record, or even transmit by a miniature transmitter what the person voluntarily tells the informer. By telling the informer something, the person has, with respect to that information, surrendered his expectation of privacy vis-a-vis the informer. Such a situation is not, of course, limited to body microphones. Telephone conversations to which one of the parties has consented and microphones installed with consent would be functionally equivalent. What is important is the consent. So long as one party to the conversation has consented to the surveillance, the other party has no justifiable

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

expectation of privacy in that which he voluntarily reveals to the party who has consented to the surveillance.[43]

Thus the absence of a reasonable expectation of privacy where one party consents to the surveillance is the equivalent of the explicit consent provision in 18 U.S.C. section 2511(2)(c).

I. "Attorney General"

Paragraph (7) defines "Attorney General" to mean the Attorney General of the United States, the Acting Attorney General, or the Deputy Attorney General. Under S. 3197 only the Attorney General or the Acting Attorney General could approve an application. The Administration had urged the Committee to permit a specially designated Assistant Attorney General to approve an application for surveillance. The Administration cites as the reason for the delegation of this authority to a specially designated assistant Attorney General the need to lessen the administrative burden of the Attorney General which would be perpetuated even after this bill has established the safeguards of a judicial warrant procedure.[44]

Some members of the Committee were troubled that the delegation of this authority as suggested by the Administration would not provide the tight control and objective methods that should be required in the foreign intelligence area. These Committee members distinguish Title III applications, for which authority may be delegated, by pointing out that: (1) Such applications are made in conjunction with specific criminal investigations and are, therefore, more capable of objective determination; and (2) that when it comes to foreign intelligence electronic surveillance it is more likely that the heads of various agencies, such as the Secretary of Defense or the Director of the FBI, will intercede directly in the application process, thus placing more pressure on the Attorney General's designate to approve the warrant request. These Committee members believe that, in the last analysis, only the Attorney General could withstand such official pressure and decide the issue in an objective manner.

Senator Kennedy maintained during the hearings on S. 1566 that since administrative inconvenience was not cited by the Ford Administration as a reason for delegating authority to review the applications, the present Department of Justice should not depart from the previous Administration's commitment.[45]

With the assurance of Attorney General Bell in his testimony during the hearings on S. 1566 that he would personally continue to approve applications under the bill until standards of review have been well established,[46] the 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.

---

[43] *United States* v. *White*, 401 U.S. 745 (1971).
[44] *Senate Judiciary Hearings*, Testimony of Attorney General Bell, pp. 18–19 (June 13, 1977).
[45] *Senate Judiciary Hearings*, pp. 18–20.
[46] *Senate Judiciary Hearings*, Testimony of Attorney General Bell, p. 20 (June 13, 1977).

J. "Minimization"

Paragraph (8) deals with "minimization", i.e., procedures which are designed to limit the acquisition, retention, and dissemination of information that is not foreign intelligence information and which relates to United States citizens or permanent resident aliens. The paragraph 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 United States persons not related to foreign intelligence. 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." [47] In assessing the minimization effort, the court's role is to determine whether "on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could to avoid unnecessary intrusion." [48] Absent a charge that the minimization procedures have been completely disregarded, the test of compliance is "whether a good faith effort to minimize was attempted." [49]

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, the degree of judicial supervision, and the length or brevity of the monitored conversations.[50] Minimization procedures may differ from case to case depending on the nature of the agency relationship, 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 specified by the judge. For example, if a citizen or permanent resident alien were using facilities of a foreign

[47] *United States* v. *Bynum*, 485 F.2d 490, 500 (2nd Cir. 1973), cert. denied 423 U.S. 1005 (1975).
[48] *United States* v. *Tortorello*, 480 F.2d 764, 784, (2nd Cir.), cert. denied 414 U.S. 886 (1973).
[49] *United States* v. *Armocida*, 515 F.2d 29, 44 (3d Cir. 1975).
[50] *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*.

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 information.

The definition of minimization speaks in terms of *acquistion*, *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 sophisticated 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 justifying the warrant, 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 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 fashioned by the court and are, of course, subject to judicial supervision.

The 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 Committee 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 could 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 fashioning the minimization order, could place 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 lawful resident aliens be handled in such a way as to assure that it is used only for the purposes specified in the definition and that it cannot be used for any other purpose. Some have suggested that the statutory definition is too general. The committee recognizes, however, that minimization requirements must differ from case to case and that minimization restrictions which are appropriate for some surveillances would be inappropriate for others. A certain flexibility in the statute is, therefore, necessary with careful judicial scrutiny of a

particular application 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 only applies to information known to concern United States 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 United States 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 United States persons.

It should be noted that this provision contains one significant change from the minimization provisions in chapter 119. Section 2518(8)(a) requires that all interceptions be recorded, if possible, and that the tapes not be edited or destroyed for ten years. In a criminal context the maintenance of such tapes and files under court seal ensures 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 Title III interceptions the very 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 more effectively safeguard the privacy of individuals, ensuring that irrelevant information will not be filed. The committee believes that existing criminal statutes relating to obstruction of justice will defer 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. § 3504, interceptions which are destroyed.

The committee is concerned that the surveillance authorized under this chapter not result in the acquisition and retention of information which would adversely affect the exercise of first amendment rights. Nor should any dissemination of the information obtained so affect those rights. Such abuses occurred with distressing frequency in the past. Information relating to the lawful political activity of American citizens or resident aliens is, by definition, not foreign intelligence information and may not be acquired, retained, or disseminated under the provisions of this legislation.

In addition to the general minimization requirements discussed above, there are two specific requirements aimed at particular types of surveillance.

The first requires that appropriate steps be taken to prevent foreign intelligence information, which relates solely to the conduct of foreign affairs, from being maintained in a way that would permit retrieval by reference to the name of a United States citizen or lawful resident alien who is a party to the intercepted communication. This requirement is intended to strike a balance between individual rights and government needs in the delicate situation where American citizens are overheard in conversations which contain information solely related to the conduct of foreign affairs.

In a hypothetical case, for example, an ambassador from an important neutral nation, speaking to a United States Senator, tells the Senator that his country has been secretly approached 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 is foreign intelligence information, the information should be retained. The alternative—a blanket rule depriving the Government of the right to retain foreign intelligence information, 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. No file should be started or maintained under the name of the American citizen when the information relates solely to the conduct of foreign affairs.

The second requirement provides special protections for permanent resident aliens and citizens of the United States who are employed by an entity controlled and directed by a foreign government or governments, which is the target of electronic surveillance and which is not substantially composed of officers or employees of a foreign government or individuals who are agents of a foreign power as defined in Section 2521(b)(2)(B). In such cases, the government must, in addi-

tion to the general procedures required by this paragraph present a statement of procedures to prevent the acquisition, retention, and dissemination of communications of permanent resident aliens and United States citizens who are not officers or executives of the entity responsible for activities which involve foreign intelligence information.

K. "United States Person"

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." This definition is new to S. 1566 since S. 3197 made no distinction in its provisions between different types of "persons." As already indicated, this new section has proven troublesome. As Senator Kennedy stated when he introduced S. 1566:

> Another major question mark concerning the bill involving the decision of the Justice Department to grant less protections and safeguards to illegal aliens or foreign visitors. This disquieting feature of the bill was absent from S. 3197. When it comes to illegal aliens or foreign visitors today's legislation provides an expanded noncriminal standard, does not allow the court to look behind the executive branch certification and allows the government to use the information obtained as a result of the surveillance for whatever purpose it deems necessary. The Fourth Amendment of the Constitution speaks in terms of protecting all "persons"—not just American citizens and lawful resident aliens—and to the extent that this bill establishing different standards and procedures for illegal aliens and temporary foreign visitors, it is open to criticism.[51]

Proponents of the change correctly point out, however, that this new distinction in S. 1566 is, in large part, the result of an Administration decision to confer additional statutory protections, over and above those found in S. 3197, for American citizens and lawful resident aliens. Thus, for example, in cases involving American citizens or lawful resident aliens S. 1566 allows the court to look behind the Executive branch certification and also expands the definition of electronic surveillance. The Committee recognizes these distinct improvements over S. 3197 and is aware of the Administration's reluctance to extend these safeguards across the board to all persons.

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. Corporations or groups which are within the definitions of a foreign power in Section 2521(b)(1) (C), (D), or (F) would continue to be foreign powers notwithstanding incorporation in the United States or the presence of a substantial number of American members.

[51] Congressional Record S7857 (daily ed. May 18, 1977).

Section 2521(b)(10) offers a new definition of "United States" for geographic purposes. Evidence publicized last year of CIA bugging 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 United States 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.

Section 2523

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

The subsection provides that none of the designated judges shall have jurisdiction to hear an application for electronic surveillance if that 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 of 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 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 ensures 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 publicly designated as the presiding judge. If the special court of review determines that an application was properly denied, it shall provide a written statement of the reasons for its decision and, 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 under this chapter shall have access to the records of actions taken by the other judges similarly designated.

Section 2524

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

Each application must be approved by the Attorney General, who may grant such approval if he finds that the appropriate procedures have been followed. The Attorney General shall also state in writing his belief that the facts and circumstances relied upon for the application would justify a judicial finding of probable cause that the target is an agent of a foreign power and that the facilities or place at which the electronic surveillance is directed are being used, or about to be used, by an agent of a foreign power, and that all other statutory criteria have been met. In addition, the Attorney General must personally be satisfied that the certification 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 interception of communications of an entire group or organization of United States 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. (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 the closest judicial scrutiny. 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 normally include such elements as methods to avoid the acquisition of irrelevant information at the time of intercept, restrictions on the use of surveillance to times when foreign intelligence information is likely to be obtained, and requirements for deletion of information obtained which is not foreign intelligence information.

For example steps should be taken to prevent unnecessary invasion of the privacy of a target's family caused by a twenty-four 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.

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" 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 the official having ultimate responsibility for the collection of the information—normally the Assistant to the President for National Security Affairs, the Director of the Central Intelligence Agency, 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 certification shall state that the information sought is foreign intelligence information, that the purpose of the surveillance is to obtain foreign intelligence information, and that such information cannot feasibly be obtained by normal investigative techniques. It shall include a designation of what type of foreign intelligence information is sought and 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 "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 ensure that those making certifications carefully consider the cases before them and avoid the temptation to simply sign off on certifications which consist largely of boilerplate language. The 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 United States 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 since the reviewing court does not have the power to control the length of the surveillance within the 90-day period otherwise applicable in the bill. This provision—a major change from the blanket 90-day limitation in S. 3197—has been criticized by some members of the committee who object to the likelihood of lengthy, ongoing wiretaps being conducted without adequate judicial supervision.

Paragraph (8) requires the application to contain a statement of the means by which the surveillance will be effected where it is not targeted against the special class of foreign powers. Unlike S. 3197, where the target is one of the special classes of foreign powers listed in section 2521(b)(1) (A), (B), or (C), the Administration has insisted that only a designation of the type of surveillance according to the categories of the definition of electronic surveillance be required. It will generally 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. The Administration maintains that 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. However, if such a surveillance requires physical entry of the property of a non-consenting person, a statement to that effect is required.[52]

Paragraph (9) parallels 18 U.S.C. Section 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. Section 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 additional facts supporting his belief that additional information of the same type will be obtained thereafter.

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

Subsection (c) enables the judge to require the applicant to furnish further information as may be necessary to make the required determinations. It parallels existing law, 18 U.S.C. Section 2518(2). Such addi-

---

[52] Some members of the Committee have expressed concern that the failure of S. 1566 to require a statement of means in cases involving the special class of foreign powers is part of a disquieting pattern, a pattern that results in less oversight of warrant applications by both the Department of Justice and the judiciary. Thus, insofar as (1) the Attorney General can delegate his authority to review warrant applications (2521(b)(7), *supra*), (2) the court has no supervisory role over the length of surveillance of "official" foreign powers (2524(a)(7)(F), *supra*), and (3) the Government need not give a statement of the means by which the surveillance of "official" foreign powers will be effected, there is obviously a marked lessening of the statutory safeguards found in S. 3197. The opportunity for abuse obviously increases. Some members of the Committee have gone along with these changes with the greatest reluctance and only because they view S. 1566—in its entirety—as a major improvement over existing law.

tional 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. Section 2518(3) and specifies the findings the judge must make before he grants an order approving the use of electronic surveillance for foreign intelligence purposes. While the issuance of an order is mandatory if the judge finds that all of the requirements of this section are met, the judge has the discretionary power to modify the order sought, such as with regard to the period of authorization (except where the special class of foreign powers is the target) or the minimization procedures to be followed.

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

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

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

In determining whether 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 surveillance is an "agent of a foreign power" under subsection 2521(b)(2)(A)(ii), (iii), or (B), the judge must, of course, find that the Government has established probable cause that each and every element of that status exists. For example, if a United States 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. There must also be probable cause to believe the person is acting for or on behalf of that foreign power and probable cause to believe that the efforts undertaken by the person on behalf of the foreign power constitute sabotage, terrorism or other proscribed activities as defined in section 2521.

Similar findings of probable cause are required for each element necessary to establish that a United States citizen is conspiring with or aiding and abetting someone engaged in sabotage, terrorism, or clandestine intelligence activities at the direction of a foreign power.

A judicial determination that a person is an agent of a foreign power as defined in section 2521(b)(2)(B)(iii) requires other find-

ings: that the person is acting pursuant to the direction of a foreign intelligence service or network; that the person is knowingly collecting or transmitting information or material to that service or network in a covert manner; and that the circumstances surrounding the activity taken together are so compelling that they indicate that the information or material transmitted to the network harm the security of the United States, or that lack of knowledge of the collection or transmission would harm our national security. Thus, the nature of the activity, its relationship to the national security, and the status of the target are all vital to the judicial determination. The required finding must be made by the judge, on the basis of the information and explanation provided by the Government. In order to determine whether the requisite probable cause has been established, the judge may request such additional information as is necessary in light of the facts and circumstances to make the required determination.

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 United States citizens or lawful resident aliens 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 prohibit dissemination of the tape. In addition, where it cannot immediately be determined 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 requirement of those sections, the court is not permitted to substitute its judgment for that of the executive branch officials. except where a United States 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 certifications 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.

Despite the fact that the court is not allowed to "look behind" the certification in cases not involving United States 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. It is this finding that constitutes a fundamental

safeguard for the civil liberties of the individual. It is also an effective external control on arbitrary executive action. Second, the certification procedure assures written accountability within the Executive branch for the decision made to engage in such surveillance. This constitutes an internal check on executive branch arbitrariness.

Moreover, it should be noted that if the description and certification do not fully comply with sections 2524(a)(7), they can and must be rejected by the court. Thus, the court could invalidate the certification if it were not properly signed by the President's designee, did not designate the type of information sought, or did not state that the information sought is foreign intelligence information, that the purpose of the surveillance is to obtain foreign intelligence information, and that such information cannot feasibly be obtained by normal investigative techniques. Further, if the certification did not present an explanation of 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, a specific definition 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 a specific definition 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. Failure to abide by the minimization procedures may be treated as contempt of court.

The order may also direct that a common carrier, landlord, custodian, contractor or other specified person furnish information, facilities or technical assistance necessary to accomplish the electronic surveillance successfully and with a minimum of interference to the services provided by such person to the target of the surveillance. If 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 the 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 authorizing judge certifying that a court order directing such assistance has been issued or, in the case of surveillance undertaken under chapter 119 or 120 in which a prior order is not required, 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 new judicial scrutiny. This period of time is not as long as some have wished but longer than others desired. It is considered to be a reasonable condition in the foreign intelligence context.[53]

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 one year without re-authorization), and this determination is not subject to the court's review or approval. As already indicated, this is a substantial change from S. 3197 which has provoked widespread criticism from some members of the Committee. The Administration, however, offers 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 Administration cites 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, as reasons for exempting these foreign powers from the 90 day limitation. Given these considerations and the unique status of the targets involved, the Administration feels that one year is not an excessive period of time.

Others disagree, maintaining that excessive paperwork and administrative inconvenience are not sufficient reasons to extend such surveillance to as long as one year without judicial approval (and with the possibility that the Attorney General will not even personally be reviewing the foreign power warrant application). Nevertheless, the

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

Committee has acceded to the Administration's position and has granted the change from S. 3197 in the limited situation of special foreign powers as defined in section 2521(b)(1) (A), (B), or (C).

In coming to this conclusion, however, the Committee emphasizes that, in order for United States citizens to be adequately protected in such cases, this provision must not be interpreted to bar judicial review of the effectiveness of the minimization procedures. United States citizens may be overheard talking to employees of such a "special" foreign power. 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 previously provided. Before the extension should be granted, however, the court would again have to find probable cause that the target is a foreign power or its agent. To aid the judge in making this determination anew, 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 was made at the request of the Administration and reflects its concern with the sensitive nature of the information obtained from special foreign powers.

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. section 2518(7). First, only the Attorney General (as defined) may authorize such emergency surveillance, whereas in 18 U.S.C. section 2518(7) the Attorney General may designate "any investigative or law enforcement officer" to authorize emergency interceptions under that subsection. Second, the Attorney General or his designee must contemporaneously notify one of the designated judges that an emergency surveillance has been authorized. There is no comparable requirement in 18 U.S.C. section 2518(7). Third, an application for an order approving the surveillance must be made to that judge within 24 hours; 18 U.S.C. section 2518(7) requires the application to be made within 48 hours. Fourth, the emergency surveillance cannot continue beyond 24 hours without the issuance of an order; under 18 U.S.C. section 2418(7) the emergency surveillance may continue indefinitely until the judge denies the application. Fifth, the Attorney General must order that minimization procedures re-

quired 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. section 2518(7). This last provision is designed to ensure that as much as possible be done to eliminate the acquisition, retention and dissemination of information which is not foreign intelligence information. The Committee's intent is to place the Attorney General in the role of the court during the 24 hour emergency period. He must examine the minimization procedures as the court would normally do under paragraph (a)(4) of this section, and order that the appropriate procedures be followed just as if he were the court granting a judicial order.

The committee wishes to emphasize that the application must be made for judicial approval even if the surveillance is terminated within the twenty-four hour period and regardless of whether the information sought is obtained. This requirement ensures 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 twenty-four hour period shall not be a basis for the court failing to enter an order approving or disapproving the subsequent application. It is necessary for both the Department of Justice and Congressional oversight committees to have available a complete record both of the bases for such emergency surveillance authorization and of the judicial determinations of their legality under the statutory standard.

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

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

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 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 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 care-

fully restricted. This section, therefore, places more stringent restrictions on use and dissemination than does the corresponding provision of Title III, 18 U.S.C. 2517. 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 seriously be 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 United States 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 the terrorist or sabotage activities 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 United States citizens and resident aliens gathered pursuant to this chapter are carefully restricted to actual foreign intelligence purposes and the enforcement of the criminal law.

A major change from S. 3197 has, however, been made in this section at the insistence of the Administration. Whereas in S. 3197 this section applied to all persons, whether or not they were American citizens, S. 1566 limits the protections of section 2526(a) to United States persons. Information concerning non-United States persons (who indeed may be foreigners not even in the United States) is not subject to the same restrictions as information concerning United States 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 United States persons and other persons was sufficiently troublesome to the Committee to result in an important amendment to section 2526(a). By limiting the subsection to United States 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 Committee has 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 committee does not intend nor does the bill permit that information gathered about a foreign visitor be used to 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-United States 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 as to whom Federal officers may disclose information concerning United States 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 carefully reviewed to ensure that there is a sufficient reason why disclosure 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, 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 United States persons. Where the information in the communication is encoded or otherwise not known to concern United States 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 United States persons is indeed present. Of course, the restrictions on use and disclosure apply to the entire Government, so that if any 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 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 such incidentally acquired information which is evidence of a crime may be retained and disclosed for law enforcement purposes. Such disclosure would, of course, be restricted by the provisions of subsection (a).

The requirement 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.[54]

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 have been minimized, that evidence would be acquired in violation of this chapter and would properly be suppressed if offered at any official proceeding.

Disclosure for law enforcement purposes must be accompanied by a statement that such evidence, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General. This provision 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).

Subsections (c), (d) and (e) set forth the procedures under the bill whereby information acquired by means of electronic surveillance may be received in evidence or otherwise used or disclosed in any trial, hearing or other 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 this subsection and the succeeding one 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.

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

Maryland,[55] and the Jencks Act.[56] 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.[57]

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 non-judicial proceedings. In instances in which the government intends to disclose surveillance information in such a non-judicial forum, subsection (c) would require that the United States 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 the intercepted communication or was a person against whom the interception was directed. Thus the word is defined to coincide with the definition of "aggrieved person" in section 2510 of title III.[58]

One situation in which such a motion might be presented would be that in which the court orders disclosed to the party the court order and accompanying application under subsection (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 subsequent 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.

[55] 373 U.S. 83 (1963).
[56] 18 U.S.C. 3500 et seq.
[57] *United States* v. *Andolschek*, 142 F. 2d 503 (2nd Cir. 1944).
[58] See also, *Alderman* v. *United States*, 394 U.S. 165 (1967).

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 referred 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 made to the defendant, as is required under Title III.[59] 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 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 subsection further provides that in making such a determination, the court may order disclosed to the person against whom the evidence is to be introduced the court order or accompanying application, or portions thereof, or other materials relating to the surveillance, only if it finds that such disclosure is necessary to make an accurate determination of the legality of the surveillance. Thus, this subsection deals with the procedure to be followed by the trial court in determining the legality (or illegality) of the surveillance.

The question of how to determine the legality of an electronic surveilance conducted for foreign intelligence purposes has never been

[59] 18 U.S.C. 2518 (9) and (10).

decided by the Supreme Court. As Justice Stewart noted in his concurring opinion in *Giordano* v. *United States*, "Moreover, we did not in *Alderman*, *Butenko* or *Ivanov*, and we do not today, specify the procedure that the District Courts are to follow in making this preliminary determination [of legality.]" 394 U.S. 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 surveillances 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 includes 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." [60]

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 excise certain sensitive portions, would damage the national security. In such situations the Government must choose—either disclose the material or forego the use of the surveillance-based evidence. Indeed, if the Government objects to the disclosure, thus preventing a proper adjudication of legality, the prosecution would

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

probably have to be dismissed, and, where the court determines that the surveillance was unlawfully authorized or conducted, the court would, "in accordance with the requirements of law," suppress that evidence which was unlawfully obtained.[61]

Where the court determines that the surveillance was lawfully authorized and conducted, it would, of course, deny any motion to suppress. In addition, the Committee emphasizes that, 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 the requirements of due process.

Subsection (f) provides for notice to be served on United States citizens and permanent resident aliens who were targets of an emergency surveillance and, in the judge's discretion, on other citizens and resident aliens who 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 ninety days upon a showing of good cause to the judge. Thereafter the judge may forego the requirement of notice upon a second showing of good cause.

The fact which triggers the notice requirement—the failure to obtain approval of an emergency surveillance—need not be based on a determination by the court that the target is not an agent of a foreign power engaged in clandestine intelligence activities, sabotage, or terrorist activities or a person aiding such agent. Failure to secure a warrant could be based on a number of other factors, such as an improper certification. A requirement of notice in all cases would have the potential of compromising the fact that the Government had focused an investigation on the target. Even where the target is not, in fact, an agent of a foreign power, giving notice to the person may result in compromising an on-going foreign intelligence investigation because of the logical inferences a foreign intelligence service might draw from the targeting of the individual. For these reasons, the Govern-

[61] The Committee has deliberately chosen the general phrase "in accordance with the requirements of law" to avoid dealing with the very complex problem of what procedures are to be followed in those cases where the trial court determines that the surveillance was either unlawfully authorized or conducted or the Government's refusal to disclose the underlying documentation to the defendant prevents the court from making that determination. The evidence obtained would not, of course, be admissible during the trial. But beyond this is the question of whether, 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 opinion in *Alderman* v. *United States, supra,* clearly answers this question in the affirmative. In the *Alderman* case, the Court 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."

Alderman, however, was a pre-title III case (which, in section 2518(10)(a) confers discretion on the court to deal with the issue of "taint" in "the interest of justice") and both this committee and the Department of Justice have maintained that *Alderman* was an exercise of the Supreme Court's supervisory jurisdiction over the lower federal courts and not a constitutional interpretation. *Senate Committee on the Judiciary,* S. Rept. 91–617, *Organized Crime Control Act of 1970,* 91st Cong., 2d sess., 64–70 (1970). However, the Supreme Court has refused to reconsider the *Alderman* rule and, in fact, reasserted its validity in its *Keith* decision. (*United States* v. *United States District Court, supra,* at 393.)

ment is given the opportunity to present its case to the judge for initially postponing notice. After ninety days, during which time the Government may be able to gather more facts, the Government may seek the elimination of the notice requirement altogether.

It is the intent of the Committee that if the Government can initially show that there is a reason to believe that notice might compromise an ongoing investigation, or confidential sources or methods, notice should be postponed. Thereafter, if the Government can show a likelihood that notice would compromise an ongoing investigation, or confidential sources or methods, notice should not be given.

Section 2527

Section 2527 requires the submission of annual reports to both the Congress and the Administrative Office of the United States Courts containing statistical information relating to electronic surveillance under this chapter. Specifically, the reports must include the 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 are 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 one 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 will provide a basis for further inquiry by appropriate oversight committees of the Congress.

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

For these reasons, the Committee believes it important that congressional oversight play an important role in the proper implementation of the statute. In that regard section 2527 must be read in the context of other congressional enactments mandating intelligence oversight.[62] This Committee contemplates that the Department of Justice and intelligence agencies will provide such information to those committees as is required by their independent oversight mandate. Indeed, it is expected that some form of Congressional oversight will be written into S. 1566 itself by the Senate Intelligence Committee when the bill is referred to that Committee. Such over-

[62] See, e.g., S. Res. 400, 95th Cong., 2d Sess. (1976).

sight would be seriously hampered if congressional committees were denied access to the information found in the application record, such as the underlying affidavits and documentation, requests for extensions, the appeal record, orders and decisions of the court.

In addition, in the exercise of its oversight function, 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 five years, or both, for each violation.

(b)(1) This amendment adds radio communication to wire communication and extends the meaning of intercept to include "or otherwise acquire" 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 sections 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. Any violation of this subsection by a carrier or its representative will render the carrier liable for the civil damages provided for in section 2520, subject, of course, to the good faith reliance defense contained therein.

(c)(1) This amendment makes explicit that an employee of the Federal Communications Commission may engage in electronic surveillance as well as intercept a wire or oral communication in 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 chapter 119 and 120 are 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."

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 ninety 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.

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. section 2511 or 47 U.S.C. section 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 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 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 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.

The activities of the National Security Agency pose particularly difficult conceptual and technical problems which are not dealt with in this legislation. Although many on the Committee are of the opinion that it is desirable to enact legislative safeguards for such activity, the committee adopts the view expressed by the Attorney General during the hearings that enacting statutory controls to regulate the National Security Agency and the surveillance of Americans abroad raises problems best left to separate legislation.[63] This language insures that certain electronic surveillance activities targeted against international communications for foreign intelligence purposes will not be prohibited absolutely during the interim period when these activities are not regulated by chapter 120 and charters for intelligence agencies and legislation regulating international electronic surveillance have not yet been developed.

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 chapter 119 and chapter 120 shall be the "exclusive means by which electronic surveillance . . . may 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.

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

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

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

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

(j) This amendment makes explicit that the reporting requirements of the Administrative Office of the United States Courts contained in this subsection 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.

COST ESTIMATE OF CONGRESSIONAL BUDGET OFFICE

OCTOBER 13, 1977.

Hon. JAMES O. EASTLAND,
Chairman, Committee on the Judiciary,
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 Committee on the Judiciary, October 5, 1977.

Based on this review, it appears that no additional cost to the government 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 ON INTERCEPTION OF ORAL COMMUNICATIONS

Sec.

§ 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 sub-

scriber 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 investigative 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 communiaction *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 communication common carrier, whose facilities are used in the transmission of a wire communication *or radio communication*, to intercept *or otherwise acquire*, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication: *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—

(I) 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,

and 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."

(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 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 extent 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 determining 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 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 communications 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 information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial, hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.]

* * * * * * *

§ 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 unobstrusively 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

§ *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 citizen or an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), who—

(i) is an officer or employee of a foreign power;

(ii) knowingly engages in clandestine intelligence activities for or on behalf of a foreign power under circumstances which indicate that such activities would be harmful to the security of the United States; or

(iii) conspires with or knowingly aids or abets any person, knowing that such person is engaged in activities described in paragraph (ii) above;

(B) *any person who—*

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

(ii) *knowingly engages in activities that involve or will involve sabotage or terrorism for or on behalf of a foreign power;*

(iii) *pursuant to the direction of an intelligence service or intelligence network of a foreign power, knowingly collects or transmits information or material to an intelligence service or intelligence network of a foreign power in a manner intended to conceal the nature of such information or material or the fact of such transmission or collection, under circumstances which indicate the transmission of such information or material would be harmful to the security of the United States, or that lack of knowledge by the United States of such collection or transmission would be harmful to the security of the United States; or*

(iv) *conspires with or knowingly aids or abets any person knowing that such person is engaged in activities described in subsections B (i)—(iii) above.*

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

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

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

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

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

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

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

(6) "Electronic surveillance means—

"(A) the acquisition by an electronic, mechanical, or other surveillance device of the contents of 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, 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 conduct of foreign affairs shall not be maintained in such a manner as to permit the retrieval of such information by reference to a United States person, without his consent, who was a party to a communication acquired pursuant to this chapter; and if the target of the electronic surveillance is a foreign power which qualifies as such solely on the basis that it is an entity controlled and directed by a foreign government or governments, and unless there is probable cause to believe that a substantial number of the officers or employees of a foreign government, or agents of a foreign power as defined in section 2521(b)(2)(B), procedures which are reasonably designed to prevent the acquisition, retention, and dissemination of communications of unconsenting United States persons who are not officers or executives of such entity responsible for those areas of its activities which involve foreign intelligence information.

(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.

(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, each of whom shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this Chapter, except that no judge designated under this subsection shall have jurisdiction of 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.

§ 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 de-

fense and appointed by the President with the advice and consent of the Senate—

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

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

(C) that such information cannot 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 description 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).

(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 affect 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.

(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 practicble, 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. 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), 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 authorization of the Attorney General.

(c) Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, 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.

(e) If an emergency employment of the electronic surveillance is authorized under section 2525(d) and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States 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.

§ 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.

MINORITY VIEWS OF SENATOR JAMES ABOUREZK

After giving careful consideration to S. 1566, the Foreign Intelligence Surveillance Act of 1977, I have reluctantly decided that I cannot support this legislation in its present form.

I have reached this decision with great hesitancy, because I endorse the goals of S. 1566—to bring electronic surveillance for foreign intelligence purposes under the rule of law and to put to rest once and for all the myth of some "inherent executive power" which, it has been alleged, superseded the clear mandate of the fourth Amendment to the Constitution.

As to the latter point, S. 1566 is clearly superior to S. 3197, its predecessor from the 94th Congress. For years, Congress has struggled with the question of a supposed inherent Presidential power in the foreign intelligence sphere. Every recent administration has claimed such a power and Congress explicitly recognized the possibility of such an inherent power when it incorporated the "national security disclaimer" in title III of the Omnibus Crime Control and Safe Streets Act of 1968.[1]

When the Ford administration proposed legislation to cover foreign intelligence electronic surveillance in 1976, it nevertheless sought to retain some vestige of this inherent power. Although the Judiciary Committee substantially amended the "Presidential Power" section of S. 3197, the bill as reported by the committee last year did reflect the demand of the Ford Administration that the proposed legislation not completely foreclose the possibility of the President exercising this supposed "constitutional power" in a narrow range of exceptional circumstances. As was noted at that time:

> It is worth emphasizing, as the congressional report indicates, that section 2528 does not constitute either a conferral or a recognition of any Presidential power to conduct warrantless electronic surveillance for foreign national security purposes. Section 2528 simply disclaims congressional intent to mandate the bill's warrant procedures in two possible situations involving surveillance by electronic, mechanical or other technical devices.
>
> * * * * * * *
>
> Given their exclusion from the warrant requirement of this legislation, the President may ultimately be found to have power to authorize each of these kinds of surveillance without judicial warrant. But even if such warrantless surveillances were constitutional in the absence of congressional action, Congress could impose a similar warrant procedure as the required mode of conducting them, just as this bill mandates

[1] 18 U.S.C. 2511(3).

> procedures for the forms of surveillance it covers. For now, however, S. 3197 defers the exercise of congressional power in regard to these additional areas of intelligence gathering.
>
> * * * * * * *
>
> In this subsection, S. 3197 stops short of asserting the regulatory power of Congress to its fullest extent.[2]

I am pleased to note that the Judiciary Committee has, this year, asserted its power to the fullest extent as regards electronic surveillance within the United States. The committee has adopted statutory language, with the full support of the Carter administration, which makes it clear that, if enacted, the Congress does not recognize any claim of inherent executive power to engage in electronic surveillance within the United States and that S. 1566 and title III of the 1968 act represent "the exclusive means" by which such activities can be conducted.

I regard this as a very positive action and commend President Carter and Attorney General Bell for their farsighted efforts in this regard.

This is not the only improvement which S. 1566 makes over S. 3197. As the committee report points out, this year's bill also brings within its scope certain targeting activities of the National Security Agency which were not covered by S. 3197. It also allows for a limited degree of judicial review of the executive certifications relating to United States citizens and resident aliens.

Again, I believe that the committee has acted wisely in adopting these improvements to the legislation.

Yet despite these positive features, I believe that S. 1566 is fatally defective in one important respect. It is the inclusion of this flawed provision that prevents me from supporting the Foreign Intelligence Surveillance Act.

I am referring, of course, to the so-called, noncriminal standard contained in subsection 2521(b) (2) (B) (iii).

For the second year in a row, the Justice Department has prevailed on the committee to include in this legislation a provision that would allow U.S. citizens and resident aliens who were not violating any federal law to be targeted for foreign intelligence electronic surveillance. This year's provision is, in fact, slightly broader than the one finally adopted by the Senate Intelligence Committee last year in that "collection" activities have been added to the definition in S. 1566.

During the committee hearings on the bill, I questioned the Attorney General closely about the need for this noncriminal standard. In addition, in response to a written inquiry he supplied me with six hypothetical cases which, he asserted, pointed up the necessity of this provision.[3]

After carefully reviewing both the oral testimony and written submissions on the question, however, I have not been convinced that this controversial provision is necessary, wise, or, most importantly, consistent with the Constitution.

---

[2] Rept. 94-1035, "Senate Committee on the Judiciary, Foreign Intelligence Surveillance Act of 1976, Additional Views of Senators Abourezk, Hart and Mathias," 94th Cong., 2d sess., 76 (1976).

[3] As an appendix, I have attached both the Justice Department's hypotheticals and an analysis of each prepared by the Washington Office of the American Civil Liberties Union.

Let me make it clear that my opposition does not stem from a belief that this noncriminal standard is overly broad. Nor do I believe that its inclusion will result in the wholesome abuses of electronic surveillance that have occurred in the past.

It is clear from any fair reading of subsection 2521(b)(2)(B)(iii) that it has been drafted as narrowly as possible.

Yet, the fact remains that this provision is in direct conflict with my belief that the 4th Amendment requires a showing of probable cause that a criminal offense has been, or is about to be, committed before an American citizen can be subjected to the pervasive type of search which electronic surveillance entails. I believe, as the Church committee found, that "as a matter of principle . . . an American ought not to be targeted for surveillance unless there is probable cause to believe that he may violate the law." [4]

Exposing Americans to such risk should be limited to situations where the alleged activity is sufficiently harmful to the national security to have been made a Federal offense.

It was principally this provision which prevented me from supporting S. 1566 in the Judiciary Committee. I believe that there is some cause for hope, however, that before this bill is scheduled for action by the full Senate, some compromise may be reached on this issue.

Attorney General Bell has already indicated that the Justice Department intends to propose statutory revisions to the espionage law intended to cover those types of intelligence activities which are designed to be covered by the non-criminal standard of S. 1566. If this were done, of course, there would be no need for subsection 2511(b)(2)(B)(iii).

A more likely short-term solution, however, might involve revising that provision of the bill so that it provides the flexibility needed by our intelligence agencies while at the same time protecting the constitutional liberties of our citizens.

I believe that such a formulation—some middle ground which will serve both purposes—can be found.

For my part, I intend to work toward that end. At the committee markup of S. 1566 on October 5, I withdrew my amendment to strike the noncriminal standard in order to provide a more neutral framework for continued discussions with representatives of the Justice Department on this matter. It is my hope that the Attorney General will be responsive to this invitation and will join us in attempting to reach some accommodation on this difficult and important issue.

---

[4] Report 94-755 "Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities, Final Report, Book II, Intelligence Activities and the Rights of Americans," 94th Congress, 2d Session, 325 (1976).

O