Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1977

LEGISLATIVE COUNSEL
FILE COPY

HEARINGS

BEFORE THE

SUBCOMMITTEE ON CRIMINAL LAWS AND PROCEDURES

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

NINETY-FIFTH CONGRESS

FIRST SESSION

ON

S. 1566

JUNE 13 AND 14, 1977

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1978

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

COMMITTEE ON THE JUDICIARY

JAMES O. EASTLAND, Mississippi, *Chairman*

JOHN L. McCLELLAN, Arkansas
EDWARD M. KENNEDY, Massachusetts
BIRCH BAYH, Indiana
ROBERT C. BYRD, West Virginia
JAMES ABOUREZK, South Dakota
JAMES B. ALLEN, Alabama
JOSEPH R. BIDEN, Jr., Delaware
JOHN C. CULVER, Iowa
HOWARD M. METZENBAUM, Ohio
DENNIS DE CONCINI, Arizona

STROM THURMOND, South Carolina
CHARLES McC. MATHIAS, Jr., Maryland
WILLIAM L. SCOTT, Virginia
PAUL LAXALT, Nevada
ORRIN G. HATCH, Utah
MALCOLM WALLOP, Wyoming

SUBCOMMITTEE ON CRIMINAL LAWS AND PROCEDURES

JOHN L. McCLELLAN, Arkansas, *Chairman*

JAMES O. EASTLAND, Mississippi
EDWARD M. KENNEDY, Massachusetts

STROM THURMOND, South Carolina
ORRIN G. HATCH, Utah

PAUL C. SUMMITT, *Chief Counsel*
D. ERIC HULTMAN, *Minority Counsel*

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

CONTENTS

	Page
Hearings held on—	
June 13, 1977	1
June 14, 1977	47
Text of S. 1566	131
Statement of—	
Bell, Hon. Griffin B., the Attorney General of the United States	12
Brown, Hon. Harold, Secretary of Defense	48
Greenhalgh, William W., Georgetown University	106
Halperin, Morton, Washington, D.C	85
Herst, Esther, National Committee Against Repressive Legislation	102
Shattuck, John, American Civil Liberties Union	74
Turner, Hon. Stanfield, Director, Central Intelligence Agency	56
Watters, David, American Privacy Foundation	111
Statement submitted by—	
Common Cause	128
Greenhalgh, William W., letter of July 1, 1977, with enclosures	122
Women Strike for Peace	129
Exhibits—	
Letter from the Attorney General, May 18, 1977, transmitting draft proposal to the Vice President	17
Letter of March 16, 1977, from Attorney General Levi, concerning the 48-hour emergency procedure in 18 U.S.C. 2518(7)	127
Letter of June 29, 1977, from Gerard V. D'Alessio, Jr., Office of General Counsel, Department of Defense	66
Questions submitted to the Department of Justice by Senator Abourezk concerning S. 1566 and response from the Attorney General	4, 5

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

HEARING ON FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1977, S. 1566

MONDAY, JUNE 13, 1977

U.S. SENATE,
SUBCOMMITTEE ON CRIMINAL LAWS AND PROCEDURES
OF THE COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The subcommittee met, pursuant to notice, at 2 p.m. in room 2228, Dirksen Senate Office Building, Hon. Edward M. Kennedy (acting chairman of the subcommittee) presiding.

Present: Senators Thurmond, Hatch, and Abourezk.

Staff present: Kenneth Feinberg, legal counsel to Senator Kennedy; D. Eric Hultman, minority counsel on subcommittee; and Mabel A. Downey, chief clerk.

Senator KENNEDY. The hearing will come to order.

Today the Senate Subcommittee on Criminal Laws and Procedures begins hearings on S. 1566, the Foreign Intelligence Surveillance Act of 1977.

This bill, which I introduced on May 18, has broad, bipartisan support and has been endorsed by the Administration. It constitutes the latest chapter in the ongoing 7-year effort to bring national security electronic surveillance under the rule of law.

The dismal record is there to examine. Seven sets of hearings on this subject have been conducted in the past 6 years; bills have been introduced only to die a slow death in committee; speeches have been made only to fall on deaf ears; inquiries made of the Executive Branch have been ignored or answered in a half-hearted way.

Last year, although two Senate committees expressed overwhelming, bipartisan support for wiretapping legislation similar to S. 1566, time ran out before the full Senate could act.

This legislation picks up where last year's left off. Using that bill as a foundation, S. 1566 builds in further improvements and safeguards. It is the culmination of past efforts and present hopes.

If the civil liberties and rights of our citizens are not to be bargained away in the name of national security, if the well-documented abuses of recent years are not to be repeated, the enactment of legislation such as S. 1566 is absolutely essential.

I am encouraged by the nature and extent of support for this bill. A major breakthrough in the debate over national security wiretapping at last seems likely.

The bill constitutes a major step forward in bringing needed safeguards to the unregulated area of foreign intelligence wiretapping.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

The legislation strikes a delicate balance between protection of national security and the protection of the human liberties and rights of the American people. It would substitute carefully prescribed accountability and oversight for the arbitrariness of the past.

S. 1566 requires that all foreign intelligence electronic surveillance in the United States be subject to a judicial warrant requirement based on probable cause.

The courts, not the executive, ultimately rule on whether the surveillance should occur. Only foreign powers or agents of a foreign power can be the subjects of a wiretap. These statutory provisions are the very heart of the legislation. They relegate to the past the protracted wiretapping abuses aimed at Joseph Kraft, Martin Luther King, Jr., and Morton Halperin. They prevent the National Security Agency from randomly wiretapping American citizens whose names just happen to be on a watch list of civil rights and antiwar activists.

The bill also mandates that before a wiretap can occur, a named executive branch official—such as the Secretary of Defense—must certify in writing, under oath, that such a wiretap is necessary in order to obtain foreign intelligence information.

The bill provides civil and criminal sanctions to those who violate its provisions.

It requires that all irrelevant information obtained as a result of a wiretap be minimized.

Before any information obtained can be used at a subsequent trial, the trial court must again find that all statutory wiretap procedures have been met, and it must provide the defendant with access to portions of the material to be introduced as evidence.

Finally, and most importantly, the bill expressly limits whatever inherent power the President may have to engage in such electronic surveillance in the United States.

In so doing, the bill ends the controversial 8-year debate over the meaning and scope of the "inherent power" disclaimer clause currently found in existing law.

The judicial warrant procedure set out in the bill, along with the detailed executive branch certification procedures, assures the type of external and internal control over wiretapping and bugging which has always been absent in this area, and which I and others have along advocated.

I candidly acknowledge that I harbor serious reservations about a few sections of S. 1566. But with the continued cooperation of the Administration, I am sure that further improvements can yet be made. That is what the legislative process is all about.

For example, we must resolve the controversial and very troublesome issue surrounding the "noncriminal standard," and the extent to which wiretapping can be authorized to investigate conduct which is not a Federal crime.

I have never been satisfied with the explanations offered to justify a retreat from the requirement of "probable cause of a crime."

Similarly, I question the provisions of S. 1566 which provide less protection to transient visitors—professors, students and just plain tourists—than to American citizens and permanent residents.

Such a distinction offends my notion of the 4th amendment, which speaks in terms of all "persons," not just American citizens.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

S. 1566 provides a double standard which constitutes a deplorable retreat from last year's bill.

Nevertheless, despite my deep reservations with a few provisions of the bill, I remain even more uncomfortable leaving the American people with no legislative protections whatever in this area. I cannot ignore the fact that today there is no judicial warrant requirement at all; that the courts currently have no role to play whatsoever in this area; and that the executive whim is uncontrolled by statute.

For too long the American people have lacked any legal safeguards to protect them against the abuses of foreign intelligence wiretapping. I believe that S. 1566 is significant, both in the bipartisan way it was drafted and in the statutory safeguards it provides.

Enactment of this bill will provide major assurances to the people of our Nation that foreign intelligence wiretapping and bugging will be conducted in the United States pursuant to strict legislative standards and accountable procedures.

I believe the time has at last arrived when Congress and the Executive together can fill the last remaining loophole in the laws governing wiretapping in the United States.

Federal law already requires that a judicial warrant be obtained before wiretapping in a criminal investigation; but no such law exists for foreign intelligence wiretaps.

With the enactment of this legislation, no wiretapping or other electronic surveillance, for whatever purpose, will be allowed in the United States, except as permitted by statute.

In that respect, I agree with Attorney General Levi's statement made in support of this bill's predecessor that such legislation "is a significant, even an historic step. I believe it is important to the country, and I hope it will be enacted quickly."

The Congress has not passed any major legislation dealing with electronic surveillance since 1968. I am confident, however, that if the deliberations concerning this bill continue to be conducted in a spirit of cooperation, a workable, just piece of legislation will be the result.

Senator Abourezk?

Senator ABOUREZK. Thank you, Mr. Chairman.

I want to make a very brief statement, if I might.

As I stated at the time that S. 1566 was introduced, I believe strongly in the purpose of this legislation. I think that you, Senators Mathias, Bayh, and Nelson are to be commended for their efforts over the past several years to produce legislation in this area.

A bill to require warrants for foreign intelligence electronic surveillance and which dispels the myth of inherent presidential power in the field is sorely needed. In some respects this bill meets that need.

I am extremely troubled, however, by a number of the bill's provisions. I think it is important that the committee examine this legislation carefully, especially in those areas where the bill differs significantly from S. 3197 of last year.

For that reason, I already submitted a detailed list of questions to the Justice Department. It is my understanding that the Department's response to those inquiries will be made available to me later this week.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

I ask, therefore, that our hearing record be left open until such time as those answers—and the answers to any follow-up questions which they generate—can be made a part of that hearing record.

I would like to join the chairman in welcoming the witnesses today.

Thank you.

[Material referred to follows:]

QUESTIONS SUBMITTED TO THE JUSTICE DEPARTMENT BY SENATOR JAMES ABOUREZK CONCERNING S. 1566

(1) Why is it necessary to distinguish between "an entity" and "an entity openly acknowledged . . ." in the definition of a "foreign power?"

(2) As to the non-criminal standard contained in 2521(b)(2)(B)(iii)—

A. In the President's statement of May 18th concerning this bill, he said that the Justice Department is now working to revise the espionage laws so that, in the future, "electronic surveillance of Americans will only be permitted when they violate the law." Can you tell us what the current status of that revision is?

B. Am I correct in presuming that when such a revised espionage statute is adopted, the noncriminal standard in this bill would be repealed?

C. Can you give the committee several examples of the types of conduct that would fall under this provision which are not also violations of the Federal criminal law;

(3) What is the reason for adding sub(iii) to the definition of "terrorism" in 2521(b)(3)?

(4) Why is it necessary to require that the targeted individual in 2521(b)(6)(A) be a "known" United States person? Known by whom? Under what standard of proof? Couldn't this provision be circumvented by targeting an individual and then simply never bothering to learn if the target is a United States person?

(5) Why was "intentional" added to 2521(b)(6)(C)?

(6) Under sub(D) of that section, the "installation" of a listening device would require a court order. Does the Justice Department regard this section as statutory authority for seeking an order to allow a surreptitious entry to make such an installation?

(7) The minimization provisions of S. 3197 had a requirement that certain information acquired from electronic surveillance be expunged from the Government's files. At the request of the Department that requirement has been dropped from S. 1566. Why did the department seek this change?

As now drafted, the bill requires that the government minimize the ". . . retention of certain information. Does this mean that some information which has been acquired, even in accordance with the minimization requirement, would not be retained? If so, how does this differ from "expunging?" If not, what is the reason for including the word "retention" in that sentence?

Does the Department foresee any contradiction between the reason for maintaining a comprehensive ELSUR index and the requirement incorporated on page 8, line 21 through page 9, line 2?

(8) Under S. 1566, only "Federal officers" may apply for a court order for foreign intelligence electronic surveillance, and then only upon the approval of the Attorney General. Can you provide the committee with a complete list of those Federal agencies and departments which would be empowered to seek the Attorney General's approval for such activities?

Would the requesting agency in all cases conduct the surveillance, or is it contemplated that one agency might conduct surveillance activities for another agency? (If the latter) How would the A.G. know which agency is actually conducting the surveillance?

(9) Regarding 2526(b)—What if information from a lawful surveillance is turned over to a local police department, that department uses the info to develop evidence of a crime, the defendant is brought to trial and then the Attorney General refuses to authorize release of the surveillance information? Must the prosecution be dismissed at that point?

(10) The conforming amendments to S. 1566 contain a detailed provision to authorize the testing of certain electronic surveillance equipment.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Would a person who is overheard and identified during a "test" have his name entered in the central ELSUR index? Would the mandatory destruction of test information deprive that person of any potential right of redress?

How many past "field" tests (as opposed to lab tests) have exceeded 90 days in length?

Would the Justice Department object to including information about testing activities in the required periodic reports to Congress?

What is the definition of "equipment being used unlawfully" in this section?

There are no time limits on this "defensive" type of testing which the bill would authorize. Are these activities on-going by nature or are they generally limited in time?

OFFICE OF THE ATTORNEY GENERAL,
Washington, D.C., June 28, 1977.

Hon. JAMES ABOUREZK,
U.S. Senate,
Washington, D.C.

DEAR SENATOR ABOUREZK: This is in response to the written questions concerning S. 1566 which you have submitted to me.

(1) It is necessary under the bill to distinguish between the two types of entities controlled and directed by a foreign government, because it is necessary to be able to secure a warrant for surveillance of certain of such entities with a warrant application which does not require as much sensitive information to be given to the judge. These entities are invariably openly acknowledged to be under the direction and control of a foreign government. In the Senate Intelligence Committee report on S. 3197 last year—where there was only one category of "entity"—the Committee stated that this category was intended to include two types of entity: an entity which appears to be a legitimate commercial establishment but which is used a a cover for espionage activities, and a legitimate foreign establishment which is directed and controlled by a foreign government and which, because of the nature of its operations, constitutes an essential source of valuable foreign intelligence information. It is normally only the latter category which would qualify for the one-year warrant. In practical terms the distinctions are justified because where there is a clandestine feature to the control and direction of the organization there is less absolute assurance of the control and direction and more likelihood that innocent Americans may be unknowingly involved, thus the bill contains the stricter requirements and shorter time periods for warrants for such entities. In contrast, where an entity is openly acknowledged to act as an arm of a foreign government, the propriety of targeting the organization should be the same as that of targeting the foreign government. The minimization standards which are the same for both warrants, and which are especially strict with respect to "entities," will assure that innocent Americans are protected.

(2) The expertise in the area of revising the espionage laws resides in the same people who are currently involved with this bill, statutory charters for the intelligence agencies, and a bill covering overseas electronic surveillance. It is, moreover, a most controversial area, and any revision will entail a lengthy dialogue within the Executive branch and within the Congress. These factors suggest that this revision will be a deliberate and fairly extended process. I cannot at this time name a date as to when the legislation would be ready for introduction, but we are already reviewing the questions involved.

We hope that this revision, when completed, would result in the repeal of the non-criminal standard in S. 1566, but I cannot reach a conclusion on that issue before our review is complete.

(3) The addition of (iii) to Section 2521(b)(3)(B) was necessary to allow electronic surveillance of persons involved in attempts on behalf of foreign powers to assassinate high Executive officials. Electronic surveillance would not be available under Title III, because the only high Executive officials protected by Federal law are the President and Vice President. Similarly, kidnapping of other high executive officials is not a federal crime unless they are transported across a state line.

(4) The word "known" in Section 2521(b)(6)(A) refers to the intelligence agency's knowledge. It is necessary because radio communications are targeted which are known to originate from or be received in the United States, but the identity of the person involved is totally unknown and largely undiscoverable.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

This activity is currently governed by Attorney General procedures to assure that it is only done in proper cases and that there is minimization of the acquisition, retention, and dissemination of the information acquired to that which is necessary for foreign intelligence purposes. These procedures would continue to apply after the passage of S. 1556. As to possible deliberate evasion of the bill's requirements by avoiding discovery of who the person is, I can assure you that a high priority of this activity is in fact to discover the identity of the communicator. If, finding that the person was a United States person, the applicable agency failed to immediately obtain a warrant—if a warrant were required for law enforcement purposes—officials of the agency would be as criminally liable as if they had otherwise engaged in electronic surveillance in violation of the chapter.

The situation may also arise where in good faith an intelligence agency is monitoring the international radio communications of a foreign governmental official who comes to the United States. Under the bill this would not require a warrant. It is possible, however, that such a foreign official could be a United States citizen. It is not unheard of for United States citizens to emigrate to a foreign country and then become an official of that country after several years. Although the law in this area is not entirely clear, generally unless an American citizen expressly renounces his citizenship, he does not lose his citizenship by becoming a citizen of a foreign country. Where this situation is known to an intelligence agency, the agency would be required to obtain a warrant under this bill if such a citizen came to the United States, but the situation has arisen where only substantially after the fact has the person's American citizenship become known. Therefore, the qualifier "known" is required to keep such a mistake from becoming a criminal offense.

(5) Intelligence agencies operating totally overseas and targeted solely against foreign communications can, through the quirks of radio communications, accidentally intercept radio communications which are intended to be wholly domestic within the United States. Over time there is a statistical certainty of this occurring at uncertain and generally infrequent intervals. Absent the word "intentional" in Section 2521(b)(6)(C), such accidental interceptions might be criminal violations when it was known that occasionally such interceptions would take place.

(6) The Department of Justice does consider section 2521(b)(6)(D) to be authority for seeking an order to allow surreptitious entry to make an installation of a listening device.

(7) The Department's language concerning minimization has always encompassed minimization of the "acquisition," "retention," and "dissemination" of information concerning United States persons which does not fit one of the statutory requirements. It has always been the Department's position that minimizing "retention" includes destruction of such information even though acquired in accordance with minimization procedures. Where agencies do not retain material, but merely pass it along, minimizing "dissemination" has included deletion of such information from what is passed along. This is, in fact, current operating procedure under Attorney General procedures pursuant to E.O. 11905. We have opposed the addition of the expunging requirement as redundant and likely to be interpreted in some unforeseen way.

The requirement that information which relates solely to foreign affairs may not be maintained in a manner permitting retrieval by reference to a United States person would prohibit the inclusion of that information in the ELSUR index, which is maintained to reply to motions under 18 U.S.C. 3504. The Department does not see this as a contradiction of the reason for maintaining the ELSUR index. The essence of a Section 3504 motion is to discover unlawful electronic surveillance for the purpose of suppressing any information thereby obtained. In practice, information retained solely for foreign affairs purposes would not be used in any trial, but rather would be used as background intelligence in our foreign relations. This amendment was inserted in the Senate Intelligence Committee last year and the Committee recognized that there are situations where information derived from United States persons incidentally intercepted is important to our foreign affairs. With this understanding, the Committee did not wish to prohibit the retention and use of this information, but to safeguard against abuse the Committee did not want that information retrievable by reference to the United States person who was a party to the communication. If the information is retrievable for Section 3504 purposes, it could

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

be retrieved for any other purpose as well, thus defeating the purpose of the Committee's amendment.

(8) I cannot provide a complete list of the Federal agencies which could request the Attorney General to seek a court order. The bill does not disable or empower any agencies specifically, nor, in my view, should it. Unlike the law enforcement field, where only certain agencies have been given authority to investigate crimes, many agencies have a need for foreign intelligence. In addition to intelligence agencies, the Energy Research and Development Agency, the Arms Control and Disarmament Agency, and the Department of Commerce, Treasury, Agriculture and other entities have legitimate need of foreign intelligence. This is not to say that these agencies directly request an electronic surveillance. At the current time, except for FBI counterintelligence electronic surveillance, other requests for electronic surveillance are filtered through various review and approval stages before they ever reach the Attorney General. The purpose of these reviews is to assess the need for the surveillance, the propriety and legality of the surveillance, whether surveillance is the least intrusive way to acquire the desired intelligence, whether the proposed surveillance will require diversion of already committed resources. Ultimately, if the request is approved at each step, the request reaches the Attorney General, who reassesses the propriety and legality of the surveillance, whether significant foreign intelligence information is sought, and whether electronic surveillance is the least intrusive feasible means of obtaining that intelligence. With the exception of FBI counterintelligence surveillance, it is probably more accurate to characterize requests as Intelligence Community requests, because, even if they originated with a particular agency, by the time the request reaches the Attorney General the request has been reviewed and approved by various components in the Intelligence Community.

(9) As a practical matter, information would not be released to local law enforcement agencies unless there had been a prior decision that the information could be used in a criminal proceeding or that the seriousness of a crime about to be committed required disclosure to prevent the crime's execution. When a prosecution is begun, if it is not possible to disclose publicly the information, it may still be possible to go forward with the prosecution because the surveillance information may be cumulative and not necessary to the prosecution. There might be cases, however, where the prosecution would have to be dismissed. This is already the situation absent the bill.

(10) A person overheard on a test would not be entered in the ELSUR index.

Destruction of test records would deprive the person of potential redress (but, of course, he would have no redress in any case unless the testing provisions were violated). This is equally true with regard to the minimization procedures requirement of destruction (i.e., minimizing retention) in intelligence surveillances. Under title III, acquisition alone is minimized, but all information acquired is recorded and retained. There are substantial policy reasons why this procedure should not be followed in intelligence surveillances. See the Judiciary Committee's report on S. 3197 at 38–39. Under title III almost invariably the surveillance will result in a prosecution and the defendants will be notified of the surveillance and may test its legality. Even if there is no prosecution the subjects of the surveillance must be notified. In addition, generally other identifiable persons incidentally intercepted are notified, see 18 U.S.C. § 2518(8)(d). Where notification is the rule, the retention of information to allow challenges is justified. Where notification is the rare exception, as it is under S. 1566, the retention of unnecessary information creates a possible source of abuse without a corresponding gain to the individual overheard, because absent notification he will not be able to test the validity of the surveillance. Both the Senate Judiciary and Intelligence Committees agree that this potential for abuse militated in favor of destruction of irrelevant information even though it resulted in the non-recording of the information for ELSUR index purposes.

I am not cognizant as to how many tests, "field" or otherwise, have exceeded 90 days. This provision originated with the Department of Defense, and it may be able to answer this question.

As to reporting to Congress on testing, again, I would suggest that you address your question to the Department of Defense.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Paragraph (ii) of the amendment of 18 U.S.C. § 2511(2)(e) does not involve testing; it involves the search for taps, bugs, and other electronic surveillance equipment used by persons in violation of 18 U.S.C. § 2511 or 47 U.S.C. § 605.

It is my understanding that such searches or "sweeps" are normally limited in time, but with especially sensitive areas they might be continuous.

* * * * * * *

I hope that these answers meet your needs. I would be happy to respond to further inquiries. It would give me great pleasure if you could fully support this bill.

Yours sincerely,

GRIFFIN B. BELL,
Attorney General.

Attachment.

APPENDIX

HYPOTHETICAL CASES

This list of hypothetical cases provides examples of situations where there is substantial doubt as to the illegality of the activity due to a lack of clarity about the reach of some current statutes; the illegality is one of state not Federal law; or, depending on irrelevant facts such as whether interstate commerce is used, the activity may or may not be violative of Federal law. Under each of the hypothetical cases, the Department of Justice believes electronic surveillance should be authorized by statute and could be authorized pursuant to section 2521(b)(2)(B)(iii).

Electronic surveillance in such cases, and others like them, should not rely on judges giving broader interpretations to Federal criminal statutes than have been applied in previous prosecutions or on the faith that judges will ignore the law and approve a surveillance when the facts are compelling. The purpose of S. 1566 is to bring electronic surveillance within the strict confines of the law, and so long as the espionage laws are not comprehensive or coherently organized, a tightly drawn non-criminal standard is required.

(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.

Stealing IBM trade secrets and research and transmitting this material to a foreign intelligence service is probably not a violation of espionage laws. 18 U.S.C. §§ 793, 794 criminalize only the collection and transmission of "information relating to the national defense." This term is not defined in the law but was described by the Supreme Court as "referring to the military and naval establishments and the related activities of national preparedness." *Gorin* v. *United States*, 312 U.S. 1928 (1941). A further gloss was put on the term by Judge Learned Hand in *United States* v. *Heine*, 151 F.2d 813 (2d Cir. 1945) where he stated that:

> It seems plain that the section cannot cover information about all those activities which become tributory to "the national defense" in time of war; for in modern war there are none which do not.
>
> * * * * * * *
>
> A less impossible interpretation would be to confine the clause to information about things adapted only for the national defense, and things of ambiguous use which have been already collected, or prepared for the supply of the armed services. The first would include airplanes, cannons, small arms and munitions of war, warships, forts, and the like; the second, coal, food, clothing or other supplies accumulated for the army and navy. Id. at 815–816.

[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.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Given this history of interpretation and the fact that the espionage laws have never resulted in the prosecution of a person for spying for purely private proprietary information, there is strong doubt whether the espionage laws would be violated by this hypothetical.

(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 officers residence, after engaging in driving maneuvers intended to shake any surveillance. Within one 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 employe of the opposite sex specializing on matters dealing with the country of the intelligence agent.

Under this hypothetical the Department of Justice believes there is probable cause to target B, but not, the State Department employee for whom there is no evidence of knowledge of B's clandestine activities. Again, there is probably no violation of the espionage laws because there is no probable cause to believe the information is "national defense" information. In fact, there is no real knowledge of what information is being collected or transmitted, but the circumstances surrounding B's activities suggests that the Government's lack of knowledge of what he is collecting or transmitting would be harmful to the national security.

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

It is not a violation of United States law to tap a data transmission line, so long as the contents are not aurally acquired. The information acquired is private proprietary information concerning components which are neither "adapted only for the national defense" nor "already collected, or prepared for the supply of the armed services." *See United States* v. *Heine, supra.* Nevertheless, knowledge of these components can pinpoint weaknesses in U.S. weapons systems and therefore can harm our national security. Nevertheless, unless the components were themselves made pursuant to a defense contract, it is doubtful whether the espionage statutes would apply.

(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.

This activity may or may not be covered under the criminal standard, depending on facts irrelevant to the threat to the national security. If D uses the facilities of interstate commerce in carrying on his bookmaking or if he fails to acquire the necessary Federal wagering license, he will violate Federal laws. So also, if his procuring involves transporting women across state lines or within the District of Columbia, he will violate the Mann Act. It is questionable, however, whether there is a sufficient nexus between these crimes and his intelligence activity to come within Section 2521(b)(2)(B)(i). In addition, it is possible that he could engage in this activity without violating any Federal law. Blackmail is a Federal crime only when things of value are obtained as consideration for not informing concerning violations of Federal law. Extortion is a Federal crime only when the means of interstate commerce are used. The customers do not violate Federal law in placing bets and engaging the services of prostitutes.

(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 United States employees of the United Nations to obtain advance information concerning United States positions in the U.N.

Burglary is not a Federal crime. Advance information concerning United States positions in the U.N. may or may not be classified and would most likely not be "national defense" information.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

(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 terriorist 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.

Infiltrations by foreign intelligence agents of U.S. organizations is not a Federal Crime. Recruiting people to infiltrate the FBI, local police organizations, and the CIA is also not a Federal crime. Presumably, at some distant point persons infiltrated into the FBI or CIA may violate the espionage laws but that occurrence is too indeterminate and far in the future to make this yet a conspiracy or attempt to commit a crime.

STATEMENT OF SENATOR STROM THURMOND

Mr. Chairman, I want to join you in welcoming our witnesses today, Attorney General Bell and Director Kelley.

It should be well noted, Mr. Chairman, the fashion in which this bill has developed. In the last Congress similar legislation was processed by the Judiciary Committee with subsequent referral to the Select Intelligence Committee. Each of these committees, with the consultation of the former Attorney General, as well as a number of Congressional leaders, carefully considered all aspects of this legislation. This process is being repeated this Congress with the goal of accommodating a number of varying viewpoints originally held and espoused by different members.

Mr. Chairman, this legislation creates a procedure for seeking a judicial warrant to authorize the use of electronic surveillance in the United States for foreign intelligence purposes. By providing such a procedure, this bill interposes a neutral, detached and independent magistrate between the executive officer and the individual.

TIMELY MEASURE

S. 1566 is a most timely bill. It strikes a proper balance between the civil liberties of the individual and the need for this nation to collect foreign intelligence information important to its security and its conduct of foreign affairs. In providing for a warrant, the bill should reassure the American public that no individual will be subject to electronic surveillance without a judicial warrant issued by an indepedent magistrate authorizing the use of such an investigative technique. In establishing a regular procedure for conducting electronic surveillance, S. 1566 insures that the government will be empowered to collect foreign intelligence information necessary for the United States to discharge its responsibilities in this modern era.

Mr. President, the bill provides that a court order approving electronic surveillance may be granted by any one of seven district judges designated publicly by the Chief Justice of the United States. It is necessary to so limit the number of judges who will have access to this critically sensitive information in order to provide proper security measures. They will be supplied not only with the names and addresses of the persons actually subject to surveillance, the compromise or disclosure of which might seriously harm our intelligence efforts, but also with information justifying belief that such person is an agent of a foreign power. Such information, if leaked inadvertently, might expose to risk or suspicion, not just a particular operation but might put informants' lives in danger or compromise unnumbered other operations by which the information as to the targets' activities was developed. Moreover, limiting the number of judges, it will be possible for a rapid growth of expertise to be developed by these judges in this very sensitive and critical area.

The case law in this area, although unsatisfactory in some respects, has supported or left untouched the policy of the Executive in the foreign intelligence area whenever the issue has been squarely confronted. Two circuit courts have held that the President has a constitutional power to engage in electronic surveillance for foreign intelligence purposes and that this power may be exercised without a judicial warrant. See *United States* v. *Butenko*, 494 F. 2d 593 (3d Cir.)

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

(en banc), *cert. denied*, 419 U.S. 881 (1974); *United States* v. *Brown*, 484 U.S. 418 (5th Cir. 1973) *cert. denied*, 415 U.S. 960 (1974). While a plurality of the Circuit Court for the District of Columbia in *Zweibon* v. *Mitchell*, 516 F. 2d 594 (D.C. Cir. 1975), stated, in dictum, that the President's power with respect to foreign powers and its agents should be exercised pursuant to a judicial warrant procedure, its holding was far narrower and was consistent with the holdings in *Brown* and *Butenko*. The court held only 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 foreign power." The Supreme Court has not directly confronted this issue, expressly reserving this question in *United States* v. *United States District Court*, the *Keith* case.

CRIMINAL STANDARD

There is no requirement in this bill, Mr. Chairman, that the target of the surveillance be actually engaged in the commission of a crime. Nor should there be such a requirement.

Our espionage statutes were written before World War I, and the nature of intelligence gathering has changed a great deal in the years since that time. Much espionage today is directed at industrial processes and trade secrets. Gathering of such information even by foreign agents for the benefit of foreign powers who are not allies, is generally not illegal. Yet the government should be able to discover these clandestine activities.

Furthermore, even activities which in their completed state would constitute crimes, in incipient stages may not be illegal. Yet, unless the government is given the tools to collect information about foreign intelligence services working at the direction of a foreign power, it may not be able to discover the completed offense.

Once again, Mr. Chairman, let me emphasize the bipartisan and widespread support that this measure has enjoyed. It is a major reform in an area of extreme complexity but of utmost importance to the survival of this nation.

Senator KENNEDY. Senator Hatch?

Senator HATCH. Thank you, Mr. Chairman.

I would like to welcome the witnesses today. It is certainly nice to have you fellows here to testify.

Senator KENNEDY. I want to point out that the distinguished chairman of this subcommittee, Senator McClellan, who is a cosponsor of this legislation and very interested in this whole subject matter, is unable to be with us but insisted that we continue to move ahead with the hearings.

We welcome two very distinguished officials of the administration, Attorney General Bell, whom we have worked with very closely in the developing and fashioning of the legislation, and Clarence Kelley, Director of the Federal Bureau of Investigation, which has important responsibilities in this area.

We welcome you both, as well as your associates, and we look forward to your testimony.

We acknowledge in these hearings, as we did in the recodification of the Criminal Code, that the administration has been extremely aggressive in working closely with us here in the Congress.

It has been personally very satisfying, and I am hopeful that this spirit of bipartisanship, the members of this committee working in close cooperation with the administration, will continue.

We look forward to your testimony. We have several areas we very much wish to pursue with you.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

JOINT STATEMENT OF HON. GRIFFIN B. BELL, ATTORNEY GENERAL OF THE UNITED STATES, DEPARTMENT OF JUSTICE, ACCOMPANIED BY FREDERICK BARON, SPECIAL ASSISTANT TO THE ATTORNEY GENERAL, AND WILLIAM FUNK, ATTORNEY, OFFICE OF LEGAL COUNSEL, DEPARTMENT OF JUSTICE, AND HON. CLARENCE M. KELLEY, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, ACCOMPANIED BY JAMES ADAMS, ASSISTANT DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Attorney BELL. Thank you, Mr. Chairman.

I hope you will tell Senator McClellan that I am sorry he could not be here. As you say, he does have a deep interest in this legislation, and I'm glad that he is willing for us to go on with the hearing even though he cannot be here.

I am pleased to appear here today to testify in support of S. 1566, a bill to authorize applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information within the United States.

There are many difficult questions involved in striking a balance between the need to collect foreign intelligence to secure the safety and well-being of this Nation and the concurrent need to protect the civil liberties of all persons in the United States and U.S. citizens abroad. Only in the last few years has this problem received the public scrutiny which it has so long deserved.

Past administrations and this administration have confronted this problem daily in dealing with particular cases without the aid of legislation to authorize that which is proper, to prohibit that which is not, and to effectively draw the line between the two.

This bill is the first step in what will be for me and many others a continuing effort to fill that void. We in the executive branch are well aware of the abuses of the past. Internal measures have been taken both by the prior administration and by this administration to assure that those abuses cannot recur.

Even if these safeguards are as effective as we believe, they have not been arrived at through the process of legislation.

This is significant for two reasons:

First, no matter how well-intentioned or ingenious the persons in the executive branch who formulate these measures, the crucible of the legislative process will insure that the procedures will be affirmed by that branch of government which is more directly responsible to the electorate.

Second, any lingering doubts as to the legality of proper intelligence activities will be laid to rest.

As you are aware, the bill before us has been the product of very close coordination between members of the executive branch representing all the affected agencies and members of this committee, the Senate Intelligence Committee, and the House Judiciary Committee.

As Senator Bayh said on the occasion of the President's announcement of this bill, this is one of the finest examples of cooperation between the executive branch and the legislative branch.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

I hope that that statement will be as accurate after the passage of this bill as it was at the time it was originally made.

I would like to ask that my statement be included in the record in full, so that I may now answer questions. I have brought two assistants with me, Mr. William Funk and Mr. Frederick Baron who have done extensive work on this proposed legislation. It may well be that they can answer some questions which I can't answer.

So they are here, and I offer them also as witnesses.

Senator KENNEDY. Your statement will be submitted into the record in its entirety.

[Material follows:]

STATEMENT OF HON. GRIFFIN B. BELL, ATTORNEY GENERAL OF THE UNITED STATES

Mr. Chairman and members of the committee: I am pleased to appear here today to testify in support of S. 1566, a bill to authorize applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information within the United States.

There are many difficult questions involved in striking a balance between the need to collect foreign intelligence to secure the safety and well being of this nation and the concurrent need to protect the civil liberties of all persons in the United States and United States citizens abroad. Only in the last few years has this problem received the public scrutiny which it has so long deserved. Past administrations and this administration have confronted this problem daily in dealing with particular cases without the aid of legislation to authorize that which is proper, to prohibit that which is not, and to effectively draw the line between the two.

This bill is the first step in what will be for me and many others a continuing effort to fill that void. We in the executive branch are well aware of the abuses of the past; internal measures have been taken both by the prior administration and by this administration to assure that those abuses cannot recur. Even if these safeguards are as effective as we believe, they have not been arrived at through the process of legislation.

This is significant for two reasons. First, no matter how well intentioned or ingenious the persons in the executive branch who formulate these measures, the crucible of the legislative process will ensure that the procedures will be affirmed by that branch of government which is more directly responsible to the electorate. Second, any lingering doubts as to the legality of proper intelligence activities will be laid to rest.

As you are aware, the bill before us has been the product of very close coordination between members of the executive branch representing all the affected agencies and members of this Committee, the Senate Intelligence Committee, and the House Judiciary Committee. As Senator Bayh said on the occasion of the President's announcement of this bill, this is one of the finest examples of cooperation between the executive branch and the legislative branch I hope that statement will be as accurate after the passage of this bill as it was at the time it was originally made.

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 guaranteee 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 affirmation of Congress that their activities are proper and necessary.

93-179 O - 77 - 2
Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Before discussing some of the more important provisions of the bill in any detail, I believe it would be helpful at this point to give an overview of the bill.

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

Approval of a warrant application under this bill would require a finding by the judge that the target of the surveillance is a "foreign power" or an "agent of a foreign power." These terms, defined in the bill, ensure that no United States citizen or permanent resident alien may be targeted for electronic surveillance unless a judge finds probable cause to believe either that he is engaged in clandestine intelligence, sabotage, or terrorists activities for or in behalf of a foreign power in violation of the law or that, pursuant to the direction of a foreign intelligence service, he is collecting or transmitting in a claudestine manner information or material likely to harm the security of the United States. The judge would be required to find that the facilities or place at which the electronic surveillance is to be directed are being used or are about to be used by a foreign power or an agent of a foreign power.

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

Finally, the judge would be required to find that a certification has been made by the Assistant to the President for National Security Affairs or a similar official that the information sought by the surveillance is "foreign intelligence information" necessary to the national defense or the conduct of foreign affairs of the United States or is necessary to the ability of the United States to protect against the clandestine intelligence, terrorist, or sabotage activities of a foreign power. Where the surveillance is targeted against a United States person, the judge can review the certification.

The bill creates two different types of warrants. A special warrant which will not require as much sensitive information to be given to the judge is only available with respect to "official" foreign powers—foreign governments and their components, factions of foreign nations, and entities which are openly acknowledged by a foreign government to be directed and controlled by that government. The other warrant is applicable to all U.S. citizens and permanent resident aliens.

The judge could approve electronic surveillance for foreign intelligence purposes for a period of ninety days except where the surveillance is targeted against the special class of foreign powers, and in such cases the approval can be as long as one year. Any extension of the surveillance beyond that period would require a reapplication to the judge and new findings as required for the original order.

Emergency warrantless surveillances would be permitted in limited circumstances, provided that a warrant is obtained within 24 hours of the initiation of the surveillance.

For purposes of oversight, the bill requires annual reports to the Administrative Office of the United States Courts and to the Congress of various statistics related to applications and warrants for electronic surveillance. The President is committed to providing to the appropriate committees of Congress in executive session such other information as is necessary for effective oversight.

Turning now to specific provisions of the bill of particular importance, I would like to point out the three specific areas in which this bill increases protections for Americans as against a similar bill proposed last year (S. 3197).

First, the current bill recognizes no inherent power of the President to conduct electronic surveillance. Whereas the bill introduced last year contained an explicit reservation of Presidential power for electronic surveillance within the United States, this bill specifically states that the procedures in the bill are

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

the exclusive means by which electronic surveillance, as defined in the bill, and the interception of domestic wire and oral communications may be conducted.

Second, the bill closes a gap that was present in last year's bill by which Americans in the United States could be targeted for electronic surveillance of their international communications. In this bill such targeting will require a prior judicial warrant.

Third, in the bill last year judges were never allowed to look behind the executive certification that the information sought was foreign intelligence information, that the purpose of the surveillance was to obtain such information, and that such information could not reasonably be obtained by normal investigative techniques. In this bill, when United States persons are the target of the surveillance the judge is required to determine that the above certifications are not clearly erroneous. While the clearly erroneous standard is not the same as a probable cause standard, it is the same basis of review which courts ordinarily apply to review of administrative action by executive officials, which administrative action may also directly and substantially impinge on the rights of Americans. We believe it is not unreasonable that where high executive officials with expertise in this area have certified to such facts, some degree of deference by the court is appropriate. This is especially so because the judges will be called upon to consider highly sophisticated matters of national defense, foreign affairs, and counterintelligence. The wide difference between such issues and the questions normally addressed by judges in warrant proceedings, conducted *ex parte* without an adversary hearing, is a major reason for adopting a standard other than probable cause.

Thus, the protections for Americans in this year's bill have been substantially increased over the protections of last year's bill.

The bill provides for warrant applications to be authorized by the Attorney General or a designated Assistant Attorney General. This provision will permit the option of eventually delegating some of the substantial administrative burden of reviewing individual case files. I am committed to personally reviewing and authorizing all electronic surveillance requests of the types covered by the bill until the bill has been signed into law and, after that, for a sufficient period to determine how the bill is working in practice and how the courts are interpreting the standards of the bill. The purpose of an eventual delegation of authority to make warrant applications would be to ensure that each individual surveillance request file receives a thorough review by an Assistant Attorney General whose time is not as constrained as that of the Attorney General. I would follow the same practice as I do now for applications for use of electronic surveillance in general criminal cases under 18 U.S.C. 2510 et seq. which are delegated to the Assistant Attorney General for the Criminal Division—I would receive weekly reports on applications authorized and refused. I would also direct my designee to consult with me on cases which present difficult policy problems in light of standards I would set for consideration of warrant applications.

In response to last year's bill a concern was expressed involving the so-called non-criminal standard for the definition of an agent of a foreign power. A United States person may be made the target of an electronic surveillance under this bill, as I have said before, only if he engages in clandestine intelligence activities, sabotage activities, or terrorist activities for or on behalf of a foreign power which activities involve or will involve violations of federal criminal laws, or if he engages in activities under the circumstances described in Section 2521(b)(2)(B)(iii) found on page 4 of the Committee print.

This so-called non-criminal standard in Subparagraph (iii) is extremely narrowly drawn. There are few, I believe, who would maintain that the activity described therein should not be a basis for electronic surveillance or even the basis for a criminal prosecution. The objection to this subparagraph, I feel, is not based upon a belief that the subparagraph's standards are too broad, but rather that as a matter of principle a U.S. person should not be made a target of an electronic surveillance unless there is probable cause to believe he has violated the law.

As a principle this is a worthy goal, but it is important to keep certain factors in mind. First, this principle is not constitutionally required; there are numerous searches which the Supreme Court has found constitutional both with and without a warrant where there is no probable cause to believe a crime has been committed. These range from administrative searches and custom searches to stop-and-frisk and airport searches. In the case of *United States* v. *U.S. District Court*

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

the Supreme Court indicated that the probable cause standard of the Fourth Amendment in intelligence searches did not necessarily mean probable cause to believe that a crime had been committed. Thus, it is our considered belief that the standard in Subparagraph (iii) is constitutional. Second, even though we might desire that the activities described in Subparagraph (iii) be made criminal, I believe that, depending upon the facts, it is possible that the activity described therein would not be held to be a violation of any current federal criminal statute. On the other hand, when a United States person furtively, clandestinely collects or transmits information or material to a foreign intelligence service pursuant to the direction of a foreign intelligence service and where the circumstances surrounding this activity indicate that the transmission of the material or information would be harmful to our security or that the failure of the government to be able to monitor such activity would be harmful to the security of the United States, then I believe that whether or not that activity is today a violation of our criminal statutes, the government has a duty to monitor that activity to safeguard the security and welfare of the nation. Third, there is a certain danger in extending the criminal law, the purpose of which is to prosecute, convict and normally incarcerate the perpetrator, merely to satisfy the principle that electronic surveillance should not be undertaken absent a criminal violation.

The Department of Justice is undertaking at this time to review the espionage laws for the purpose of making them comprehensive in the areas in which prosecution is warranted and generally to rationalize this area of the law. This undertaking is quite difficult, as illustrated by the fact that the controversial espionage provisions of the former S. 1 were the result of just such an undertaking. I can only assure you today that we will do our utmost to draft revised espionage laws in such a way that the non-criminal standard might be repealed.

Another issue which has been the cause of some concern is the treatment of non-U.S. persons; that is, illegal aliens, foreign crewmen, tourists, temporary workers, and other aliens not admitted for permanent residence. Director Kelley will present to you persuasive reasons why the facts require different treatment for such persons whose contacts with or time within the United States is likely to be extremely limited. I would like only to make the point that it is our considered view that such differing treatment wholly conforms to the Constitution. There is no doubt that the Fourth Amendment protects aliens in the United States as well as United States citizens. And under this bill a prior judicial warrant is equally required for all aliens within the United States, whether permanent residents or not. The standards for this warrant are slightly different for certain aliens, however. The bill reflects generally a distinction between different types of persons or entities; that is, the showing for a foreign power is less than for a natural person; the showing for an alien who is an officer or employee of a foreign power is less than that which is required of other aliens; and the showing required for non-resident aliens is less than that for United States persons, which includes resident aliens. There is a rational basis for each of these distinctions, and this is sufficient to assure that the differing standards do not violate the Equal Protection Clause. Therefore, we believe this differing treatment is wholly in accord with the Constitution of the United States.

There have been some questions raised as to what agencies of the United States Government would be involved in electronic surveillance under the bill and what if any change this would mean from current operating procedures. I do not believe that this bill would make any change in which agencies would in fact conduct electronic surveillance or receive its product. Generally only two agencies would be engaging in electronic surveillance under this bill and that would be the FBI and the National Security Agency. Which agency would be involved might depend on various factors, including the nature of the target, the purpose of the surveillance (whether the purpose was for positive foreign intelligence or counterintelligence), and the type of electronic surveillance involved. The respective military services would have the power to engage in electronic surveillance for counterintelligence purposes on military reservations. The CIA is, of course, barred from conducting electronic surveillance within the United States. There is, however, a large degree of cooperation and coordination between the various intelligence agencies on particular electronic surveillances. For example, the need for a particular electronic surveillance might come from the State Department, the CIA might be the agency who had developed the particular equip-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

ment to be used, the FBI might be the agency to in fact conduct the electronic surveillance, the product of the surveillance might go to another agency for analysis, with only the analyzed product then going to the State Department. The bill does not make any specific limitations on which agency may conduct electronic surveillance, and I do not believe that such a limitation would be advisable. Not only are the organization, structure, and duties of the intelligence community subject to some change, but the development of capabilities and technologies by differing agencies cannot be accurately predicted in advance. There will of course be restrictions on the dissemination of information obtained from electronic surveillance not only for security purposes but also to comply with the minimization procedures that the court would order. Again, I do not believe specific limitations as to specific agencies would be advisable in the statute itself.

There is, I know, a desire on the part of several members of both this Committee and the Senate Select Committee on Intelligence to extend statutory protections to Americans abroad who may be subjected to electronic surveillance. This desire is shared by this Administration. The Justice Department, in coordination with members of the various affected intelligence agencies, is actively at work on developing a proposed bill to extend statutory safeguards to Americans abroad with respect to electronic surveillance for intelligence or law enforcement purposes. There are, however, special problems involved in overseas surveillances, some of which arise out of the fact that the United States' legislative jurisdiction is limited overseas. In the next several months, again after close coordination with interested Members of Congress, we expect to be able to present proposed legislation on this subject.

In closing, I would urge that this bill be swiftly enacted into law as a significant first step toward outlining by statute the authority and responsibiliy of the Government in conducting intelligence activities.

OFFICE OF THE ATTORNEY GENERAL,
Washington, D.C., May 18, 1977.

The VICE PRESIDENT,
U.S. Senate,
Washington, D.C.

DEAR MR. VICE PRESIDENT: Enclosed for your consideration and appropriate reference is a legislative proposal to require a judicial warrant for all electronic surveillance within the United States conducted for foreign intelligence purposes. This proposal is designed to make unlawful the kinds of abuses of national security electronic surveillance that have occurred in the past, while clearly establishing the legality of electronic surveillance for intelligence purposes in limited circumstances.

Last year, similar legislation was reported favorably by the Senate Committee on the Judiciary and the Senate Select Committee on Intelligence. This proposal would, however, go beyond the protections afforded to U.S. citizens and permanent resident aliens in last year's bill in three major respects: First, the proposal ensures that persons in the Unittd States cannot be targeted for electronic surveillance without a judicial warrant. Last year's bill did not extend the warrant requirement to NSA "watch listing" of American citizens. Second, the proposal contains no reservation of any inherent power of the President to conduct electronic surveillance for intelligence purposes without a judicial warrant. Third, whenever a United States person is targeted for electronic surveillance, the proposal authorizes judicial review of the Executive's certification that the information sought is foreign intelligence information.

The submission of this proposal by no means terminates the Administration's commitment to a thorough and continuous review of intelligence practices and procedures. This review will move forward in close consultation with interested members of Congress. Work is already in progress to draft legislation safeguarding the rights of Americans outside the United States in connection with electronic surveillance for both intelligence and law enforcement purposes, an area of concern not covered by the enclosed proposal. In addition, the Administration is beginning a review of the espionage laws currently in force, with an eye toward eventual revision and modernization of those statutes. At such time as the espionage laws are rewritten in a manner which effectively criminalizes hostile intelligence activities without jeopardizing First Amendment freedoms, it may be possible to eliminate even the extremely limited provision in the enclosed proposal which permits surveillance of U.S. persons engaged in acts which are not

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

clearly prohibited by current criminal law. Finally, the Administration is committed to providing the appropriate committees of Congress with all information necessary for effective oversight of intelligence activities by the Legislative Branch.

This proposed legislation is needed to fully assuage public fears of the potential for abuse in electronic surveillance for intelligence purposes, and to provide officers and employees of the Executive Branch with definite guidance as to the range of permissible activities. I, therefore, urge the early consideration and adoption of this legislative initiative.

The Office of Management and Budget has advised that enactment of this legislation would be in accord with the program of the President.

Yours sincerely,

GRIFFIN B. BELL,
Attorney General.

Attorney General BELL. In response to what Senator Abourezk said, we are preparing answers to your questions, and we will prepare more answers after you have had a chance to see these.

Senator KENNEDY. First, as I mentioned in my opening statement, the members of this committee and other members as well have been very interested in this area for at least the last 7 years, especially since the decision in the *Keith* case and its relationship to the 1968 Safe Streets Act. How are we going to deal with the problem of foreign intelligence wiretapping has been a matter of great concern to this committee.

There has been a series of legislative proposals which I, Senator Nelson, Senator Mathias, Senator Hart, Senator Bayh, and Senator Abourezk, and many other Members, have introduced over the last few years.

So the importance of addressing this issue is recognized both by you and the Administration. I think what is extremely important to recognize is that by not acting, by not passing legislation, a policy decision is nevertheless being made. And that policy is based on complete Executive discretion.

So it is extremely important, I think, that we move ahead.

There are some special areas that we have been interested in that were addressed in the course of the legislation last year. This year, we have reached different conclusions on certain issues.

The first area I would mention you relate to in your own testimony on page 9 where you indicate:

"I am committed to personally reviewing and authorizing all electronic surveillance requests of the types covered by the bill until the bill has been signed into law and, after that, for a sufficient period to determine how the bill is working in practice and how the courts are interpreting the standards of the bill.

"The purpose of an eventual delegation of authority to make warrant applications would be to ensure that each individual surveillance request file receives a thorough review by an Assistant Attorney General whose time is not as constained as that of the Attorney General."

In the bill of last year, it was clear that:

The Attorney General means the Attorney General of the United States or, in his absence, the Acting Attorney General.

Yet you state in your testimony on page 7 that:

The Attorney General means the Attorney General or an Assistant Attorney General, specifically designated in writing by the Attorney General.

We understood, at least in the bill last year, that this matter was of such sufficient urgency and sufficient importance as to require the

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Attorney General of the United States to personally sign off on each application.

I see a modification in this year's bill.

I am wondering whether there would be any reason why we couldn't go back to the original language of last year's bill—whether you would have any reservation.

Quite frankly, what disturbs me is your prepared testimony, which will become the legislative history, that suggests "whose time is not as constrained as that of the Attorney General."

Some could read that as indicating that this whole area does not have the priority of other areas.

I think those who recognize the importance of this issue believe that the Attorney General should be the one who personally signs off on this.

I am interested in your reaction.

Attorney General BELL. The bill last year represented the views of Attorney General Levi. He spent, as he told me, about 50 percent of his time on intelligence matters.

He believed, and I may well have believed that last year myself, that at that time in our history that the Attorney General should handle it personally.

After I came to Washington, I found that I was spending a great deal of my time on the same sort of matters, plus handling title III wiretaps.

Under the law, title III surveillance requests can be delegated, and I have delegated that to the Assistant Attorney General in charge of the Criminal Division. On a weekly basis, he gives me a report as to any matter he has handled under title III.

I think the day will come where it would be better to have an Assistant Attorney General assigned strictly to intelligence matters but under the supervision of the Attorney General—maybe on a weekly basis. Otherwise I can see the day coming when the Attorney General will spend all of his time on intelligence matters, and the 54,000 employees will not have anybody looking after what they are doing in all the other areas of the Justice Department. This takes a lot of time.

I can understand your worry. You want to hold somebody responsible, and you view this as a serious business—as do I. You would rather have the Attorney General do it.

I am perfectly willing for the bill to be amended, if that's what the wisdom of the Senate is. I will carry it out.

Senator KENNEDY. It is not only this, General Bell. This relates, of course, to the other provisions of the legislation relating to the noncriminal standard.

In title III, we are talking about violations of laws; we're talking about crimes. But in this bill we're talking in some of noncriminal areas, of noncriminal standards which I think put an even higher requirement on the attention of the Attorney General.

Second, I don't think we have to imagine very far down the line when you are going to assign these applications to a very capable and able, bright, sensitive, and concerned assistant. But you may very well find that the Secretary of Defense or the Director of the FBI

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

will personally indicate their strong belief about a particular issue or question relating to the coverage of this particular legislation.

It seems to me that the Attorney General should be the one that addresses those concerns and at that level. If it comes from the Director of the FBI or perhaps the head of the CIA or the Secretary of Defense, the Attorney General himself should negotiate.

I don't know how many assistants—although I am sure there are some—who would be able to resist successfully, the very powerful and well-intentioned suggestions that would be made by other high-ranking officers in the executive department.

I think that in this area there are different requirements than title III. This is why I believe it is so essential and important to mandate the direct involvement of the Attorney General.

Attorney General BELL. There is a good deal to what you say, Mr. Chairman.

Certainly, if there is going to be an Assistant Attorney General handling intelligence matters, the Senate should know about it in advance so they can test him thoroughly when he appears for confirmation.

I don't object to your doing that.

Senator KENNEDY. We require that, as a matter of fact, under the bill with respect to the certification. Whoever is going to be designated would first have to be confirmed with the advice and consent of the Senate.

Attorney General BELL. This legislation is so important to the Nation that I wouldn't want to see it held up on account of who is going to be responsible. I would rather say I would be responsible than see the legislation held up.

But I want the committee to know that it takes a lot of time. And I am held responsible for many things.

Senator KENNEDY. The application for the warrant must include a statement of the means of surveillance.

In last year's bill, we require on page 17 the means by which the surveillance will be effected.

It seems to me, in reviewing the legislative history on this, it would be extremely important to know both the technical means of the type of electronic surveillance and also the means by which that particular surveillance would take place.

In the legislation this year, on page 14, you indicate that:

> 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), or (B), or (C), a designation of the type of electronic surveillance to be used according to the categories described in Section 2521 (b)(6).

There is an important distinction here. You are just asking for the type of surveillance—whether it is going to be a bug or wiretap—and last year's bill not only includes that, but also requires a description in terms of the means that will be used.

I think that is an important distinction, and I would like to direct your attention to that change which I find troublesome.

Attorney General BELL. We are willing to include the language, "and whether physical entry will be used to effect the surveillance."

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Senator KENNEDY. We will take a look at that particular language.

The third area is on page 22 of last year's bill, in terms of the time requirements: "An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose or for 90 days, whichever is less."

In your proposal, you have an order "under this section shall approve electronic surveillance targeted against a foreign power," and it has the references to sections, "for one year or whichever is less."

So we are getting an extension of the time period by 9 months.

I know, obviously, that you have the problem of bureaucratic factors and the rest, but there is a significant difference, I think, between the 90-day period which was established, and the 1-year period, which is suggested in this legislation, particularly when you realize that included in the coverage of foreign powers will be Americans. I am wondering about that.

Attorney General BELL. That, I think, is a reasonable provision, because it says 1 year or less and can be controlled by the Attorney General in the court.

There are different types of activities, as the chairman knows. There would be some matters where you would want to have an order for 1 year—many would be for less. It depends on the type of activity, which I should not go into detail here in public. But I think it is a reasonable requirement.

Senator KENNEDY. If you had a particular kind of government that you were wiretapping—and it's been going on for 30 years or whatever—you could do it year in and year out over any period of time.

But it seems to me having that kind of requirement, in terms of 90 days, does not really burden you in terms of the administrative or bureaucratic rituals that would have to be followed.

I don't know, just offhand, in giving thought to this particular requirement, why the 1 year is to be preferred to the 90 days.

Attorney General BELL. Speaking for the Department of Justice and the FBI, we can live with 90 days.

Senator KENNEDY. Alright.

Attorney General BELL. But I suggest there may be some other witnesses who will want to explain——

Senator KENNEDY. We'll have a chance to get into that tomorrow, but I wanted to get your views.

Attorney General BELL. We can live with the 90 days. That generates a good deal more paper where you have repeated requests, but there may be some other witnesses who would explain the 1 year.

Senator KENNEDY. Can you live with 90 days, Mr. Kelley?

Director KELLEY. We would like to have the opportunity to think about extending it.

Senator KENNEDY. You will let us know your views?

Director KELLEY. Yes.

Senator KENNEDY. If you could give us your view on that it would be helpful.

Attorney General BELL. This legislation is the product of all the intelligence agencies. I think you will find some others who would like to have an ear.

Senator KENNEDY. In the area of the noncriminal standard, I'm sure you are very familiar with the problem. We've talked about this

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

privately and during the confirmation hearings and have gone through it in very considerable detail during the negotiations over the bill. This is a very troublesome area; why you think the existing espionage law is insufficient to cover the kinds of situations the noncriminal standard is designed to reach.

I understand the administration is working on a revision of the espionage laws. But that is still some distance down the road and will require a good deal of negotiation with various Members of the Congress. We look forward to working closely with you in that area.

I am sufficiently concerned about the danger which continues to exist without this legislation that I am willing to move S. 1566 even with the noncriminal standard.

In our bill of last year, concerning the definition of the noncriminal standard, some of the protections that we had are absent in this bill. For example, we were not only talking about Americans at that time, because you had a noncriminal standard that applies to all "persons."

It is my belief that when you are talking about the noncriminal standard, the same standard should apply to all persons—not just Americans.

In the definition of your noncriminal standard, you have substantially taken the same noncriminal standard that was eventually worked out in the course of last year. Fine.

But in the provisions of your legislation you have diluted a noncriminal standard that applies to other non-Americans. I am referring to that particular section.

You have in your legislation: "Knowingly engages in clandestine intelligence activity for or on behalf of a foreign power under circumstances which indicate such activities would be harmful to the security of the United States."

In the provision that applied to that same group of persons last year, we had: "A person acting pursuant to the direction of an intelligence service or intelligence network which engages in intelligence activities. And in a manner intended to conceal the nature of such information or material or the fact of such transmission under circumstances which would lead a reasonable man to believe information used to harm the security of the United States."

It seems to me that the provision in our legislation this year is a significant retreat in terms of protections. It troubles me.

If we're talking about the fourth amendment and the noncriminal standard, we are talking about "persons," not just citizens.

Granted, the definition which is used this year in terms of Americans, is essentially the same which was used last year. But as to other "persons" it is not.

I am interested in gaining your reaction, because in this area, we are talking about movement—in the wrong direction frankly—from the legislation of last year.

Would you comment on that?

Attorney General BELL. The language you read is still in the bill but under another section. It applies to any person.

But the section you are directing your remarks to is what we call the foreign visitor standard.

Senator KENNEDY. Exactly.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

That's important.

Attorney General BELL. We have receded from the standard of last year in the sense that it is a lesser standard—less stringent. We think that we have addressed this problem. Director Kelley can give more facts on this than I can.

I can say that with a foreign visitor, the problem is a serious problem in some circumstances. We think this standard is adequate.

Senator KENNEDY. You are right in reminding us that we are not talking about the standard that would be applied to Americans. The standard which is included in our legislation concerning Americans is not different from what we had last year. It has the protections that I mentioned which would virtually prohibit the excesses that existed during the Watergate period.

We are not talking about how that standard could be applied. I think it's important we understand that. But we are talking about non-American persons who come here to visit.

I would be interested if you might indicate why if we use the same standard for all persons, as the fourth amendment does, Americans as well as visitors, what additional hardships you believe would result.

Attorney General BELL. We are not willing to extend the fourth amendment protection to an officer or employee of a foreign power—a person who is knowingly engaged in clandestine intelligence activities for or on behalf of a foreign power or conspires with or aids or abets someone doing those things. We don't think we should extend the fourth amendment protection to those people.

We think it would be a hardship on the Bureau if we did.

There are large numbers of people involved in some areas, and I think Director Kelley can tell you about that.

Senator KENNEDY. Would you like to elaborate, Director Kelley?

Director KELLEY. Going from 1961 to 1977, the number of Communist-bloc officials permanently assigned was 518 in 1961 and 2,298 in 1977; Soviet bloc cultural and commercial visitors, 5,439 in 1972 and 10,337 in 1976; Soviet crewmen 1,300 in 1972 and 40,234 in 1976; Soviet tourists, 1,128 in 1973 and 1,747 in 1976.

Senator KENNEDY. How many did you have last year? You didn't have that many more last year—and we didn't have this provision in the bill last year.

What has changed in terms of the nature of the threat?

Attorney General BELL. Maybe you're dealing with a different set of people.

Senator KENNEDY. I agree.

Attorney General BELL. I think there is something wrong if we are trying to extend the fourth amendment fully to people who come here and meet this definition. After all, the fourth amendment does not extend fully to you or me if we are at a border in a customs matter.

So there are varying levels of fourth amendment protection, and I think this is adequate, myself. I don't think we should treat somebody from another country better than we treat our own people.

Senator KENNEDY. That's right. But, of course, we are talking about Americans who are going to be contacting or talking to them. There will be Americans who will be affected.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

It was the recommendation last year by Attorney General Levi, that this wasn't considered an undue burden by the Ford administration.

So I am interested in why you feel that the situation has been altered or changed and what are the additional new threats from visitors from Eastern European countries or the Soviet Union that present the need for this change. We obviously want to find out the justification for the change.

Attorney General BELL. This is my judgment of what the law should be. I am well satisfied with this standard.

I think when you couple this with the minimization procedures that we use, where some of these people happen to be talking to American citizens, we have to present the case on minimization to the judge and we have to make certain that we minimize any constitutional intrusion.

So it seems to me that all that fits together, to me, pretty well.

Senator KENNEDY. Since we are talking about the nature of the surveillance—both on Americans and non-Americans—General, and from your testimony here—you indicate that as of June 9, 1977, nationwide there were only 77 subjects of telephone and 3 subjects of microphone surveillance in operation in FBI cases, and none of these subjects were U.S. citizens. Is that correct?

Director KELLEY. Right.

Senator KENNEDY. There are no U.S. citizens that are at the present time, subject to electronic surveillance for foreign intelligence purposes? Am I correct?

Director KELLEY. No citizen is targeted.

Senator KENNEDY. Does that mean the same thing? We are used to different meanings of words, particularly in this area.

I know you don't mean to be vague, and I've never had a problem, with all due respect, with you. You speak very frankly in language that I understand. But just so that we do understand—we don't have any American who is now being electronically surveilled for foreign intelligence information. Is that correct?

Director KELLEY. I was using the word "targeted" in the sense that the authority is on someone who is other than a citizen.

There are, of course, others from time to time, and that's what I was talking about in saying "targeted."

Senator KENNEDY. Fine.

As to foreign nationals or foreign aliens or however we describe those who come to this country other than American citizens, there are 77?

Director KELLEY. That's right.

Senator KENNEDY. For foreign intelligence purposes.

Director KELLEY. That's right.

Senator KENNEDY. Can you indicate to me, General Bell, which agencies or departments of the Government seek Justice Department approval for the wiretaps?

Attorney General BELL. Any agency can apply, but I receive everything from the FBI and the NSA part of the DOD. I speak in initials now, like everybody else. [Laughter.]

Everything comes through the FBI.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Mr. ADAMS. We also get requests initially, and have in the past, from the CIA.

Senator KENNEDY. I will come to that.

As I understand it, your answer is that any request that you receive comes from the FBI to you.

Attorney General BELL. Right.

Senator KENNEDY. Director Kelley, could you tell us what agencies make requests of you for foreign intelligence surveillance?

Director KELLEY. The Department of Defense, the Department of State, the CIA, and NSA.

Senator KENNEDY. The CIA, as I understand it, is prohibited in its charter from performing electronic surveillance in the United States. Are they contracting this out to you? [Laughter.]

Director KELLEY. No.

Mr. ADAMS. We do have matters of mutual interest where a case begins overseas under the jurisdiction of the CIA. The individual may come to the United States, and it is basically within our counterintelligence responsibility. But we are advised of it by the CIA, and there is a handoff of the particular investigation.

Senator KENNEDY. Do you return that information all to the CIA?

Mr. ADAMS. Yes.

Senator KENNEDY. What is the internal procedure that you follow in making a decision—whether you grant the request or do not grant the request?

Mr. ADAMS. When we receive a request, for instance from NSA or any of the other agencies, after they have gone through the deliberative bodies in other agencies, then they come to us. We prepare the justification, indicating the basis for the wiretap and prepare a memorandum for the Attorney General's approval in which we indicate the manner in which the surveillance will be enacted—whether it involves a trespass or not—and then forward it to the Attorney General for his approval under the delegation of powers.

Senator KENNEDY. Do you sign off? Have there been requests made which you have rejected?

Mr. ADAMS. Yes; there have been requests in the past that have been rejected.

I remember one in particular that was rejected.

Senator KENNEDY. We are interested, obviously, in the procedures—whether you are applying independent judgments on these matters or whether you are merely a funnel in terms of various agency applications to the Justice Department. Whether you are making independent decisions, how those decisions are made, and the procedures that you follow—but we will get into that with you later through a more detailed series of questions.

Attorney General BELL. I might say that I don't know how many Mr. Kelley and Mr. Adams reject, but I reject some they send to me. And a number I have sent back for additional information.

Senator KENNEDY. Just as a final question, could you tell us at what stage is the Justice Department's effort to come up with a comprehensive charter for the FBI?

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Attorney General BELL. The working committee which worked on this particular legislation we are discussing today is now working on a charter. They just started within the last 2 weeks.

We are working on it, and Congressman Edwards is also working on it. Eventually the Senate Intelligence Select Committee will be working on it.

I am most anxious to get started on it. I don't want to leave the impression that we are dragging our feet.

Senator KENNEDY. When do you expect that we'd see that?

Attorney General BELL. If you'd put on a deadline, it would help me.

If you were to say a month from now. If I haven't gotten something on it in a month, I may write it myself. [Laughter.]

Senator KENNEDY. Do you believe a charter would be important?

Attorney General BELL. It is most important. I would say it is the most important matter facing the Bureau.

Senator KENNEDY. What do you think, Director Kelley?

Director KELLEY. I agree completely. It's a very important thing.

Senator KENNEDY. Senator Thurmond?

Senator THURMOND. Mr. Attorney General, we are glad to have you with us. I want to commend you for the outstanding job you've been doing as Attorney General.

Attorney General BELL. Thank you, sir.

Senator THURMOND. Judge Bell, S. 1566 differs from last year's S. 3197—by eliminating an express reservation of the President's inherent powers to engage in electronic surveillance in matters outside the definition of electronic surveillance and, also, for matters that could not be reasonably said to have been within the contemplation of Congress.

Is it your position that even though this language is deleted from the bill, the inherent presidential power is preserved as interpreted by the courts?

Attorney General BELL. Yes. Because we can't change the Constitution.

But this is an accommodation between the legislative and executive branches of the Government where the President has agreed that he will follow the provisions of this statute in matters inside the United States.

I repeat: We can't change the Constitution by agreement.

Senator THURMOND. S. 3197—last year's bill—contained a unique provision which precluded this specially designated judge from looking behind the executive branch certification. This certification feature has been dropped from S. 1566.

Do you believe this change is procedurally sound in view of the responsibility of the executive branch to certify that the information sought is information necessary to the national defense or the conduct of the foreign affairs of the United States?

Attorney General BELL. I do.

This looking-behind process only applies in matters where American citizens are involved. We think the clearly erroneous standard is an adequate basis for proceeding. I'm not worried about that. I think it probably enhances the bill. You ought not to have the judge acting without some discretion in the matter.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

So I am well-satisfied with that. That was the change we made.

Senator THURMOND. S. 1566, this year's bill, creates a special warrant for official foreign powers, which permits a warrant for 1 year and with less-sensitive information than would be required for a standard warrant directed against U.S. persons.

The question is: Do you feel that the more restrictive standards for U.S. persons is well justified?

Attorney General BELL. I do. I think that there is a rational basis for the distinction. You ought to have more strict standards where American citizens' rights are involved. We think that that is a reasonable approach.

Senator THURMOND. Director Kelley, under S. 1566 the minimization procedures required shall not preclude the retention and disclosure for law enforcement purposes of any information which constitutes evidence of a crime, if such evidence is to only be used in a criminal proceeding, with the advance authorization of the Attorney General.

Do you believe this standard is reasonable with regard to your responsibilities to enforce certain criminal laws?

Director KELLEY. I believe that it is reasonable.

Senator THURMOND. Director Kelley. As you know, the bill before us provides for two kinds of warrants—special warrants for foreign powers and standard warrants for U.S. citizens.

The standards for U.S. citizens are more restrictive than for foreign powers.

Do you see this difference as a problem to the effective electronic surveillance of U.S. persons engaging in activity threatening our national internal security?

Director KELLEY. I do not think that is a problem.

Senator THURMOND. That's all, Mr. Chairman.

Senator KENNEDY. Senator Hatch?

Senator HATCH. As I understand it, the bill provides for seven district judges designated by the Chief Justice of the Supreme Court of the United States to make these determinations.

First of all, is that enough judges?

Attorney General BELL. I think it is.

The reason I think it is a sufficient number is because I am handling all of them myself now, so if we get seven people doing what I do, that would be about right. [Laughter.]

Senator HATCH. I would have to agree with you.

Is there any loss of security in working with the seven judges? Do you anticipate any security leaks, and are there any provisions concerning the activities, actions, and approaches that the judges have to take?

Attorney General BELL. The most leakproof branch of the Government is the judiciary.

Senator HATCH. Or the most leaky.

Attorney General BELL. No. The courts have a great record in this area. I'm not worried about them. I have seen intelligence matters in the courts.

Although we don't have the seven designated judges, about the only problem is: Do they have safekeeping measures?

If we have seven judges, of course, we can arrange all that. It would be difficult to arrange it for 500 judges, but I think seven will work out.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

I have great confidence in the courts. It might be because I used to be in the courts.

Senator HATCH. I do also.

Senator THURMOND. Mr. Chairman, I am on a conference for military procurement, so if you would excuse me I must leave.

Senator KENNEDY. We could keep you here and not get your vote on the B–1 bomber. [Laughter.]

Senator HATCH. I don't think anybody could keep him anywhere from having the B–1 bomber.

Senator KENNEDY. That's what I am afraid of. [Laughter.]

Senator HATCH. I'm concerned about whether this bill is inadequate in the sense that it might open an opportunity for third parties to come in; for instance, when denial is made and there is an appeal to the circuit to a special three-judge court of review and then to the Supreme Court. Is there any chance for third parties to come in and disclose the security nature of the surveillance procedures?

Attorney General BELL. It is ex parte.

It would be hard for a third party to get in.

Senator HATCH. My question is: Is this bill tightly enough drafted so that it will remain ex parte right up to the Supreme Court of the United States of America?

Attorney General BELL. We think so.

Senator HATCH. Would you advocate that it has to be?

Attorney General BELL. I think it has to be ex parte. I don't know of any other way to do it. You couldn't have a hearing with these backed up in papers for these sensitive warrant applications. I would have to just quit and withdraw the request.

Senator HATCH. So you don't anticipate this becoming anything but an ex parte proceeding without interference by special interest groups that may or may not like electronic surveillance?

Attorney General BELL. No. We couldn't function. It would compromise the system. I would have to say: No; we will back out and withdraw the request.

Senator HATCH. If we could have this procedure screwed up by people coming in anytime they want to question the procedure, I think you would have a very difficult time having any security with regard to the procedure. Isn't that correct?

Attorney General BELL. You would.

What we always have to have in mind is that we don't have any judicial protections now.

What this bill does is to afford the American people protection from the judicial system, but it will be ex parte.

Senator HATCH. Director Kelley, if you would like to comment on any of these matters, feel free to do so.

Director KELLEY. I will.

Senator HATCH. With regard to the 90-day provision, you indicated, Director Kelley, that you could live with that. Do you really feel that it is adequate, or do you feel that you need a more lengthy period of time in order to utilize the effectiveness of this particular statute?

Director KELLEY. In the case of the 90-day renewal need, of course, as is true now, we would come in and ask for a renewal. We have lived with it to date, and we could live with it in the future. We only thought

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

from the time of the deliberations that a 1-year continuation or less, if indicated by the activities, that it might well be better to go 1 year.

It is a matter of just not having the necessity to go the four times as compared with one time in the 1 year.

But we can live with the 90-day provision if it is felt that this is the better system by you and the Department.

Senator HATCH. We are trying to find out what is the best system.

I think that the legislature should be concerned about what is the best, the most efficient, and the fairest system that we can possibly devise and still maintain the security of this country.

The way I am interpreting you, and correct me if I'm wrong, is you can live with the 90 days but you would certainly prefer it to be 1 year rather than have repeated returns to the court to get the very same thing you would need anyway.

Director KELLEY. Senator, I'm trying to abide by what is actually best for the country, plus the fact that we want to have clearly defined our intention to do that. If it be better understood as properly restrictive in a very sensitive area, we can go with the 90 and will.

As a matter of perhaps expediting or trying to have less of a burden in going through the continuations, we could go for 1 year. But I say we are in a crucial period; we are trying to do this in the best manner possible; 90 days would be my decision right now.

Senator HATCH. In other words, if the decision was 90 days, you could live with it, but you would prefer a year. How long does the average surveillance take? Is it less than 90 days or more than 90 days?

Attorney General BELL. Let me say something here.

The 1 year only applies to official foreign powers. The 90 days is to citizens.

Senator HATCH. Right.

Attorney General BELL. I'm hoping you will leave us with 1 year. I don't think it would be good to answer the question of how long an average surveillance goes on.

Senator HATCH. That's fair. I'll withdraw that question.

But would you, General, prefer 1 year also then?

The way I am interpreting both of you, it would be more expeditious and beneficial to national security to have 1 year in this particular case rather than 90 days.

Attorney General BELL. On foreign power.

Senator HATCH. Right.

Attorney General BELL. We don't ask for more than 90 days on individuals. We think they should be reviewed every 90 days.

Mr. ADAMS. Senator, the reason for that is that foreign intelligence gathering is a long-range proposition. This isn't something that starts one month and ends the next month.

When we are dealing with foreign powers and foreign establishments, we are dealing with historical trends that have taken place over many years.

You may not come up with something during the 90-day period or even a 6-month period.

So the reason for the 1-year, basically, is because of the long-range nature. By restricting it to a foreign power, as such, it was felt that

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4
93-179 O - 77 - 3

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

this would not be a controversial issue because of the very nature of the recognition that these foreign powers are engaged, and have been engaged, in hostile activities against the United States for many years duration.

Senator HATCH. Is there any effort being made in the Government at all, in any area of the Government, to require reciprocity and fair treatment by other countries for U.S. citizens?

In other words, we seem to be doing all these great things for foreign nations. Are we requiring any nations to do anything for us in this area?

Attorney General BELL. Not that I know of. I'm not familiar with any effort being made to have a treaty on this sort of thing.

Senator HATCH. Are there any efforts being made to include this as part of our human rights approach?

Attorney General BELL. Just a moment. I want to confer with my assistants.

Senator KENNEDY. You think the cruise missile is going to be tough to enforce; I would think this one is going to be worse.

Senator HATCH. That's right. But it is always nice to try because esoteric concepts sometimes change the whole world don't they?

Attorney General BELL. I was wondering not long ago if I could file a suit for an injunction against foreign powers conducting certain intelligence activities in the United States. It would be the first time anybody used that process in intelligence, but nobody seems to think that would be worthwhile.

Senator HATCH. I would think that if the United Nations is worth anything, we should be able to at least use it as a matter of public record; that human rights are involved here; this country is recognizing domestic as well as foreign human rights; therefore, we would like to have that same reciprocity from other people throughout the world, even though it may be difficult to monitor.

Attorney General BELL. It may be that the day will come when we will have that kind of progress. This would be a very good step here—where we are not only protecting the rights of American citizens, but we are giving foreign visitors rights as they come in. Even a foreign power knows what the law is. If we go by the law, we not only do it in the executive branch but we get the imprimatur of the court on what we do.

Senator HATCH. In essence, General, we have always done that more than any other nation, haven't we?

Attorney General BELL. And now we have taken one further step to show our respect for the individual liberties.

Senator HATCH. I think it is a forward step.

Mr. ADAMS. In that connection, it also relates back to a question from Senator Kennedy as to why at this hour we are raising the question concerning treating foreign visitors differently than U.S. citizens.

In dealing with any type of legislation, in particular something as sensitive as national security, you don't just sit down at the table and come up with all the ideas at once.

As this thing progressed, we on the investigative side of the FBI became more aware of the potential problem of treating visitors as

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

restrictively as U.S. citizens. Our experience in this regard develops from the fact that we see certain countries—in particular, the Soviet Union—directing individuals in this country in the student exchange program, foreign visitors of all types, and the Soviet seamen—each group penetrated by hostile intelligence officers. They serve as an extension, or an arm, of the Soviet government in this regard.

They are totally unlike a U.S. citizen who is in this country and has had an obligation of loyalty over the years and dedication to the principles that have made America great.

These individuals, we have seen, penetrate every group. We have seen everyone utilized, either as a full-time intelligence officer or as a cooptee team for a one-time mission. This is why we felt, and went to the Department and raised concerns which we have from an investigative standpoint, that when the number of Soviet seamen in the United States jumped from 1,300 one year to 13,000 the next and 40,000 last year, our resources are limited in dealing with this type of group.

They are not within the United States for a lengthy period of time. It does require some latitude and extraordinary coverage in order to attack these particular groups from an intelligence standpoint.

We have seen them not only in the United States but in other countries where the same techniques are used to penetrate these delegations with intelligence officers.

Senator KENNEDY. Why don't you go get them under the espionage laws?

I'm all for getting them, but it seems to me we should do it under the espionage laws.

Mr. ADAMS. It's a question if we had the probable cause in order to make an arrest under the espionage laws, we really wouldn't need that same degree of cause in order to put on a wiretap.

What we are dealing with is an historical fact that in some of these official delegations that not only the temporary but the permanent ones—where 40 percent of them have intelligence assignments—and we have only identified 28 percent, say, of a particular group, that we need——

Senator KENNEDY. How many cases have been brought against aliens?

Attorney General BELL. Against foreign citizens?

Senator KENNEDY. Yes. How many have you documented and how many cases have been made against these individuals?

Mr. ADAMS. For prosecution?

Senator KENNEDY. Yes.

Mr. ADAMS. Very few.

The primary purpose of counterintelligence work is to neutralize the activities of these groups to prevent their intelligence-gathering activities, and hardly any of them wind up in prosecutive action.

Most of them have diplomatic status which prevents any prosecution action whatsoever. Even those where we have made the case because they were assigned to the United Nations where they had no diplomatic status, because of particular deliberations going on at that time, we were unable to obtain prosecution.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Senator KENNEDY. So what are you asking them to do is leave this country?

Mr. ADAMS. That's right.

Senator KENNEDY. How many have we asked to leave?

Mr. ADAMS. I don't have——

Senator KENNEDY. I'm trying to find out the range.

We had this similar trend last year. Yet we had an Attorney General who drew different conclusions from what this administration has drawn.

It seems to me we should find out whether there has been an additional threat which is posed to our security interests.

I agree that reasonable men can look at the situation and draw different conclusions.

What we are inquiring into is why you made the decision this year but not last year. Then, if the case is made for expansion, I would be interested in what you are doing about it—whether you are deporting and the extent of it. I think that would be helpful to us.

Senator HATCH. General Bell, do you have additional comments?

Attorney General BELL. I was just going to answer that question.

As I see it, what we have done here for foreign visitors is enough. We have a serious problem here in counterintelligence in trying to keep up with all these people that are being sent in here to engage in this kind of activity. I, for one, am not willing to give them all the rights that an American citizen has. American citizens haven't even had these rights until now.

We are proposing that we do this to safeguard American citizens.

But I'm not willing to change the foreign visitors' standard. In answer to the question, I would just have to say that our views are different from the people who were pushing this bill last year.

Senator HATCH. I don't care if it is 10,000 people you throw out of the country or 1, that 1 may be the most important person to throw out we have ever seen. It may be worth every bit of intelligence effort that you have made.

Mr. ADAMS. It's not like a criminal case. You are dealing with the most sophisticated activity in the world—a spy. He has the resources of a foreign country behind him. He has the technological advances, unlimited funds, the military establishment and the diplomatic establishment. These are the most difficult cases to cope with.

Senator HATCH. Is it always propitious to bust a spy?

Mr. ADAMS. No; we frequently don't.

Senator HATCH. In fact, in many cases, it is more propitious to identify him so you can work within that framework of intelligence.

Mr. ADAMS. We try to recruit him after we catch him. We would like to have him work our side of the street. If we can't do that beforehand, we try to identify his contacts and see who in the Government is transmitting this classified information to him or who in private industry that has contracts with the Government in classified areas. So it isn't just a question of prosecution. It is the total counterintelligence effort.

Senator HATCH. It is a pretty complex area, and the security of this country needs to be protected as well.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Attorney General BELL. You have to have in mind also that we are now engaged in this type of activity without a statute and we need to know what it would be like to add this layer of protection by the judiciary. We have to have some workable system. We think this bill is a workable system.

If it turns out later on we can afford more safeguards, we will be glad to do that. That's our business. The Department of Justice is charged with safeguarding the rights of people.

We won't be trying to hold back; we will be trying to afford more safeguards.

Right now, we think this is about right at this time.

Senator HATCH. Thank you, Mr. Chairman.

Senator KENNEDY. Senator Abourezk is not a member of this committee, but he is very interested in this area and has worked closely with us and the administration on it.

Senator ABOUREZK. Thank you.

Mr. Attorney General, in your statement today, and also in the President's statement accompanying the bill on May 18, it was said that the Justice Department is working to revise the espionage laws so that in the future "electronic surveillance of Americans will only be permitted when they violate the law."

Can you tell the committee what is the status of that revision and when we might expect draft legislation from the Department?

Attorney General BELL. I am going to let Mr. Baron answer that, because he has been preparing the answers to your written questions.

Mr. BARON. We are proceeding with the attempt to consider revisions of the espionage laws. The problem is that the expertise in the Justice Department on espionage and counterintelligence questions, and civil liberties concerns involved therein, resides in the same group of people who have been drafting this bill and who are also drafting the intelligence charters legislation.

So we can't move as fast on all fronts at once, but we are trying to go as fast as we can.

Senator ABOUREZK. What's your estimate of when we will have a draft?

Mr. BARON. We are just starting to talk in terms of the time limit on charters today. I'm afraid that even if we get something drafted on charters, there will be a period of several months of intense negotiations back and forth within the executive branch and with Congress before we finalize charters. The revision of the espionage laws will probably be the next item of business after that.

Senator ABOUREZK. So you can't give an estimate?

Mr. BARON. I think it would be unrealistic to name a date.

Senator ABOUREZK. If and when such a revised espionage statute is adopted, would I be correct in assuming that the noncriminal standard in this legislation would then be repealed at the behest of the Justice Department?

Mr. BARON. That would be our hope.

It is a very difficult business to revise the espionage laws, as we saw with the attempt in S. 1 last year. We are hoping to be able to come up with a revised espionage law that would relieve the need for a noncriminal standard in this bill.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Senator ABOUREZK. So your aim is to repeal the noncriminal standard as soon as you can define everything in an espionage statute that you think needs defining to collect wiretap information? Is that correct?

Mr. BARON. That is our present intention.

Senator KENNEDY. Could I get that from Attorney General Bell?

Attorney General BELL. That's our present intention to do that.

Senator ABOUREZK. The bill's definition of minimization procedures in section 2521 requires that the Government minimize the retention of certain information.

Does this mean that some information that is acquired during the course of the surveillance would not be retained; that is, it would be destroyed?

Mr. FUNK. My name is Bill Funk, and I am also working on the response to your questions, which are usually very pointed and well drafted and take some expertise.

Yes; definitely information is obtained which is then destroyed.

Under the existing procedures of the Attorney General, you try to minimize acquisition; but, just as in the criminal field, you can't absolutely stop the acquisition of irrelevant information. Some slips by. When it slips by, here are existing requirements which we would expect to continue under the minimization procedures in the bill to destroy that information which did not fit the specific categories of what could be retained and used.

With the minimization of "retention," that means destruction.

Senator ABOUREZK. Do I understand that this legislation does not preclude retention of some materials under the minimization procedure for use in a criminal prosecution? Is that correct?

Mr. FUNK. That's one of the specific bases on which you can retain things under the bill. It specifically states that the minimization procedures do not stop the retention of material that can be used as evidence of a crime.

Senator ABOUREZK. Based on that, my question is: If you go in under the noncriminal standard and obtain a wiretap order or warrant, can you then, under this legislation, use the evidence in a criminal prosecution?

Mr. FUNK. Yes; theoretically you could, just as under title III you can presently get a warrant for one criminal activity but if you gather evidence of another criminal activity, you can use it.

Senator ABOUREZK. But under title III, it is a criminal standard. We are talking about something different here.

If you go in under the noncriminal standard of S. 1566 and if you acquire information, retain it and then use it in a criminal prosecution, isn't that a violation of the fourth amendment?

Mr. FUNK. No, sir, I don't believe it is. The Supreme Court has said in the home welfare searches that if a person is legally in a place, with the right to be there, then what they see within their plain view can be used—even though the basis for their being there in the first place was not a criminal violation. This was true in *Camara* against *Municipal* Court, as well as the case of the welfare home visits where there was no criminal violation involved but if you were in there legally, then you could use something that you did find.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Attorney General BELL. One of the hardest questions you face is where you are legally getting information, and you might accidentally overhear or find out some crime has been committed by a high official of the Nation. Are you to ignore that, or should you prosecute the high official? That can easily happen.

Senator ABOUREZK. The same thing would be true——

Attorney General BELL. You are not just talking about the rights of some downtrodden person. We are talking about some high person who might be picked up.

Senator ABOUREZK. What if you, as Attorney General, walked into somebody's home and barged in without a warrant at all? Would you be entitled to prosecute if you saw——

Attorney General BELL. We are talking about electronic surveillance and not going into somebody's home.

Senator ABOUREZK. It doesn't matter. We are talking about search and seizure under the fourth amendment.

Attorney General BELL. I know a lot about the fourth amendment, and I'm not going to barge into anybody's house.

Senator ABOUREZK. It's the same thing as doing it if you go in under a noncriminal standard and get a wiretap order and then collect criminal evidence against somebody.

Attorney General BELL. We would be going in under a standard set and defined by the Congress. That is a legal standard.

Senator ABOUREZK. Yes; but we haven't set that yet.

Attorney General BELL. I know you haven't yet.

Senator ABOUREZK. That's what we are considering here today.

Attorney General BELL. Suppose we are doing it now in foreign intelligence under the Constitution. There is no safeguard now at all except the discretion of the executive—assuming that they carry out their oaths.

Senator ABOUREZK. There is very little safeguard under the noncriminal standard, so you are not adding very much.

Attorney General BELL. You are adding as much as you have now on an American citizen who comes through customs, where you only have to have a reasonable suspicion.

Senator ABOUREZK. I think that might be considered a different circumstance.

The American citizen voluntarily leaves the country, and he voluntarily comes back. But he doesn't voluntarily agree to being wiretapped.

He might be deemed to have subjected himself to a search when he reenters the country if he leaves it. The same thing is true of going to an airport, where you consent to a search before boarding a plane.

Attorney General BELL. We wouldn't do this to the average American citizen. We would only do it to one who was acting pursuant to the direction of an intelligence service or an intelligence network of a foreign power who knowingly collects or transmits information or material to an intelligence service or an intelligence network of a foreign power in a manner intended to conceal the nature of such information or material or the facts 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

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

lack of knowledge by the United States of such collection or transmission would be harmful to the security of the United States.

So that is the standard. That is not just some frivolous conduct. You would have to meet that standard. That is a fairly severe standard.

Senator ABOUREZK. You are aware, of course, of section 794 of title 18 of the United States Code, which is the espionage statute?

Attorney General BELL. Yes.

Senator ABOUREZK. Do you consider what you just read broader or narrower than section 794.

Attorney General BELL. I can't answer that question because I don't have it in front of me.

We will answer it in writing, however.

Senator ABOUREZK. To follow up on that, my question is: Why don't you rely on the espionage law instead of trying to restate the espionage law? Why do you need a noncriminal standard?

Attorney General BELL. We have said that we are going to study the espionage statutes and try to offer an amendment later, if we can accommodate our needs to the espionage statute as amended.

Senator ABOUREZK. Would you be willing to support a self-destruct provision in this legislation that the noncriminal standard would be automatically repealed at the end of 1 year or 18 months after enactment of this legislation?

Attorney General BELL. I'm not certain that I would, because I don't think that, as Attorney General, I could destroy evidence of high crime —or any kind of crime.

Senator ABOUREZK. We are not asking you to do that. We are asking you to get rid of the noncriminal standard—not the criminal standard.

Attorney General BELL. I don't understand your question perhaps: but if I find out that there is some crime which has been committed through this surveillance, which began under this standard I have just read, and I pick up information that a crime has been committed, I will have to do something about that. I couldn't destroy it.

Senator ABOUREZK. You don't believe that is unconstitutional to do that?

Attorney General BELL. I would let the court pass on the constitutionality. I wouldn't make that judgment.

If I find that some crime has been committed, I would try to do something about it.

Senator ABOUREZK. But they haven't ruled on this section yet.

Attorney General BELL. The court?

Senator ABOUREZK. Yes.

Attorney General BELL. Not yet.

Senator ABOUREZK. That's what I'm saying.

Attorney General BELL. I would go by the court's instructions.

Senator ABOUREZK. Is it your view that the noncriminal standard in this legislation is designed to overrule or circumvent specific judicial decisions interpreting the current espionage law?

Attorney General BELL. I will let Mr. Baron answer that.

Mr. BARON. I think the problem is that the judicial constructions of the current espionage laws are not yet complete enough and clear enough for the executive branch to be sure that they reach all forms of

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

espionage that need to be covered. That is the reason for the non-criminal standard.

There are certain modern forms of espionage, like industrial espionage, which are not clearly under the reach of the current criminal espionage laws.

Senator ABOUREZK. Would you answer the question.

Is it designed to either circumvent or overrule those decisions?

Attorney General BELL. Not that I know of. That's the first I've heard that we are trying to circumvent any court decisions.

Senator ABOUREZK. Your answer is, no.

Attorney General BELL. No. To the best of my knowledge.

Senator HATCH. As I understand, what you're saying is that there are certain examples, such as foreign espionage to acquire trade secrets, information about industrial processes, foreign personnel facilities located in the country, et cetera, that do not constitute a crime but may be vital to our national interest.

You don't want to give up the right to have that information or to expunge a record or to self-destruct that record do you?

Attorney General BELL. You are right; that is our view.

Senator HATCH. And that's what you are saying today. So I think maybe that does answer your questions, Senator Abourezk.

Senator ABOUREZK. I'm sorry. I didn't hear your answer.

Senator HATCH. I think that does answer your question a little more specifically.

Senator ABOUREZK. What does?

Senator HATCH. That there are certain acts that do not rise to the nature of a crime under our present criminal laws but necessarily become essential to our security interests in this country.

Senator ABOUREZK. What would those be?

Senator HATCH. I just read them off: Foreign espionage to acquire trade secrets, information about industrial processes, foreign personnel and facilities located in the country, terrorist activities, sabotage——

Senator ABOUREZK. Terrorist activities and sabotage are crimes.

Senator HATCH. But the others are not crimes.

Senator ABOUREZK. Why not include those as criminal activities then?

Senator HATCH. I think maybe we ought to, but the fact is right now they're not.

Senator ABOUREZK. It is just as easy to do that as it is to pass this law.

Senator KENNEDY. Rather than our imagining, could we ask them?

Senator HATCH. I did, and they said that they agreed those were important aspects.

Senator KENNEDY. If you would just review with us the kinds of activities you would consider under this——

Attorney General BELL. We have a hypothetical case we could give you if it would help any.

Mr. BARON. We have prepared several hypothetical cases in response to Senator Abourezk's written questions. This is one of them, and we will submit others in writing to you later.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

It is intended to illustrate an area where it is not clear that the current espionage laws would reach.

The hypothetical is a situation where a reliable informant reports that a U.S. person has, pursuant to the direction of the KGB, collected and transmitted sensitive economic information concerning IBM trade secrets.

The U.S. person—and here we mean an American citizen or a permanent resident alien—is placed under physical surveillance and is seen to fill dead drops which are cleared by a member of the Soviet Embassy, known to be a KGB agent.

On the second Tuesday of every month, the U.S. person drives around the Soviet Embassy, after engaging in driving maneuvers intended to shake any surveillance. While driving around the Soviet Embassy, coded CB transmissions are sent from the Soviet Embassy.

The U.S. person has a CB receiver in his automobile. This activity is not clearly prohibited by current U.S. law.

Senator ABOUREZK. What was the information that he was going to transmit to the KGB?

Mr. BARON. That is precisely the problem.

What you have here is what you have in most espionage cases. I'm sure that Jim Adams can respond for the FBI as to the way these cases are usually developed.

You have a set of circumstances where it is almost crystal-clear that there is espionage activity going on, and there is a U.S. person involved. But under the current espionage laws, it is very difficult to ensure that there is "national defense information" that is in, perhaps a coffee can being put down by a KGB agent and picked up by a U.S. citizen.

It could be IBM trade secrets involving our most sophisticated computer technology, which might have relevance to weapons technology.

Senator KENNEDY. You must have a better illustration. If he is working with the KGB agent, isn't that conspiracy to commit espionage?

Mr. BARON. No. The problem is, with the current espionage laws, he is clearly in league with somebody who works at the Soviet Embassy but it is not clear that current law would nail him, because the current law requires a showing that national defense information is involved. And it is not clear enough that something like IBM trade secrets that might relate to weapons technology—which is not officially classified—is national defense information under the statute.

Senator KENNEDY. Even with a KGB agent, you don't think you can convince a court?

Mr. BARON. That is the problem. We would be in a posture of not knowing whether we could convince a court or not. With the noncriminal standard in the law, as we propose it, it makes it clear that when you are involved in this kind of conduct, you ought to be covered. Presumably, in a revised espionage law, you would be covered.

Senator ABOUREZK. May I get back to the minimization procedures and destruction of irrelevant material?

Can you tell the committee under what circumstances that destruction would occur?

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Mr. FUNK. Destruction would occur normally as soon as the information was obtained. In other words, as soon as it slipped by the acquisition. You are supposed to turn off the recorder as soon as you determine that it is somebody you are not targeted against or it is innocent information.

There are a lot of cases under title III and under the criminal standard where initially you have to get some sense of the code they are talking in. So you might listen for a couple of days just to get a feel for what the information was, and then you would go back after that and take out that information that was irrelevant.

So you would have destruction both at the time and later.

Senator ABOUREZK. Who would make the decision on whether or not to destroy certain materials?

Mr. FUNK. I can only state what current procedures would be which I would imagine would all be spelled out in the minimization procedures approved by the court itself.

Under present procedures, it is done initially by the person on the scene. It is reviewed by people further up the ladder and further deletions or destructions are made, and then there is oversight by reports to the Attorney General on a yearly basis. And here it would be 90 days to the courts.

Senator ABOUREZK. If an individual is overheard on electronic surveillance and subsequently all material relating to that interception is destroyed, would that person's name be entered in the Department's central ELSUR name index?

Mr. FUNK. No; it would not.

This was a hard policy decision last year with S. 3197. This is no change from last year's version.

In both the Judiciary Committee and the Senate Intelligence Committee, they agreed due to the differences between a law enforcement surveillance and an intelligence surveillance. Under title III, people who are overheard are notified——defendants are notified; even people who aren't defendants are notified by the court.

Here notification is a very rare situation.

When the Government has in its files names and information and tapes of peoples' communications, which those people are never going to be notified about, we should only be holding that if we have a good, legitimate, necessary interest in the Government to utilize that information.

To keep this merely because someday it might be required for an ELSUR index request for a 3504 motion would increase the potentiality for abuse. We think the potentiality for abouse outweighs the necessity because it is so unlikely that the information will be called for. If it is irrelevant, we should get rid of it and destroy it. It won't be used.

Senator ABOUREZK. Mr. Attorney General, obviously some of the technical answers have to be given by your staff, but for the record and for legislative history, do you adopt those as your answers unless you correct them?

Attorney General BELL. I do.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

These men are on the working group which produced the bill. They have had many, many meetings with other people in the intelligence community on this subject. I have to rely on them.

Senator ABOUREZK. That's fine with me. I just want to make sure, for legislative history, those are your answers as well.

Attorney General BELL. I work very closely with them.

Senator ABOUREZK. On page 27 of the legislation, I want to refer to the section beginning with line 10 where it is provided that it is lawful for an officer, employee, or agent of the United States to conduct electronic surveillance for the purpose of testing electronic equipment.

There are certain limitations on the time and the duration of testing, and so on.

You can do this, as I read the legislation, without a warrant. Is that correct?

Mr. FUNK. Yes, sir.

Senator ABOUREZK. Why do you want to test equipment on people without a warrant?

Attorney General BELL. You really are not testing it on people, so much as you are testing it.

Senator ABOUREZK. You are overhearing conversations.

Attorney General BELL. Usually in a test you would, and that's why you have to destroy what you pick up.

Senator ABOUREZK. If you want to provide protection for the American people, why wouldn't you want to provide them protection of a warrant for the purpose of testing? Why can't you test whatever equipment you want to test alongside the existing equipment for which you have obtained a warrant?

Attorney General BELL. There is not a target when you are testing.

Senator ABOUREZK. What if you decide to test some new equipment on Mort Halperin, for example?

Attorney General BELL. We're not going to do that. [Laughter.]

Senator ABOUREZK. That's what the last group said. [Laughter.]

Mr. FUNK. I think it would clearly be a violation of the bill and it would be subject to all the criminal sanctions therein. Perhaps we can tighten the language to make clear that you are not testing against individuals.

When you talk about testing alongside other equipment or why don't you test when you have a warrant, that's not really the problem here.

We're talking about the equipment that the U.S. Army may use in wartime; that it sends overseas to be used in case we're attacked. It may be something that would only be used against Soviet fighter aircraft, or something.

But when we are in the United States, and we have a contract, we have to test to see if it works. If you test it against American fighter aircraft and the equipment doesn't work too well, you may pick up some other things and then calibrate to make sure they're only on the right frequency.

Senator ABOUREZK. Do you need a warrant to conduct surveillance against an airplane?

Mr. FUNK. No. The point is that we'll get other things as well, and you'll have to calibrate the equipment so that you will get other things

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

as well, and then you'll calibrate it down so that you only get the fighter aircraft.

Senator ABOUREZK. Are you talking about just equipment that will listen in on airplanes? Is that all you're talking about?

Mr. FUNK. We can't talk about all of it. We are talking about this as a substantial part of it.

Attorney General BELL. This is sophisticated equipment. It is not one for surveillance of a person.

Senator ABOUREZK. Why don't we put that in there then? Why do we leave it wide open?

As I read the bill, you can test it on anybody without a court order.

Attorney General BELL. We might be able to tighten that up.

Senator ABOUREZK. It's a wide loophole.

Attorney General BELL. I know what this is.

Senator ABOUREZK. The thing is that you don't want to test it on somebody's telephone or put a bug in somebody's home, or whatever.

Attorney General BELL. We don't; that's right.

Senator ABOUREZK. So why don't we say that?

Attorney General BELL. We'll see if we can tighten it up.

Senator ABOUREZK. I think the committee might want to take a closer look at that.

Attorney General BELL. I think sometimes we know what these things mean, and maybe we don't articulate them as well as we should.

Senator ABOUREZK. There is a requirement for certification by two or three people—the National Security Adviser and a couple of others.

As I read this legislation there is no penalty for fraudulent certification. Does it come under the statute for swearing falsely? Can you respond to that—if they do swear falsely?

Mr. FUNK. It would definitely be a violation of 18 U.S.C. 1001.

Attorney General BELL. Making a false statement. You don't have to swear—just make the statement. Section 1001 is sort of a catchall.

Senator ABOUREZK. Are you saying that there is a violation if you just make a false statement without bothering to swear to it?

Attorney General BELL. Oh, yes. That's the law now.

Senator ABOUREZK. You'd have everybody in Washington in jail. [Laughter.]

Attorney General BELL. The fact is there are a considerable number of people in prison for doing that. [Laughter.]

Senator ABOUREZK. You haven't got the right ones.

Attorney General BELL. We don't have everyone. [Laughter.]

Senator ABOUREZK. Under title III of the criminal wiretaps statute, the general practice has been that the agency which initiates the application for electronic surveillance is also the agency that actually conducts the surveillance.

For example, if the FBI applies for an order in a gambling investigation and the order is granted, the FBI will be the only agency involved in the conduct of the surveillance operation.

It is my impression that this independence between agencies is not so clear in the foreign intelligence field. Is it your view that under this bill the requesting agency would in all cases conduct the surveillance, or is it contemplated that one agency might conduct activities for another agency?

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Director KELLEY. We will have requests made of us to make an installation, coming as it might from the Department of Defense or the CIA, but we are the ones actually who are in the role of requestor, and we are the ones who conduct the surveillance and the ones who record the results.

Senator ABOUREZK. In Attorney General Bell's statement on page 15, you state that the bill does not make any specific limitations on which agency may conduct the electronic surveillance.

You say, also, that you do not believe that such a limitation would be advisable.

Does that mean, in your interpretation of it, that the CIA, for example, could conduct domestic electronic surveillance?

Attorney General BELL. No, sir; they can't do that in the United States.

Senator ABOUREZK. You mean not legally.

Attorney General BELL. I have a new way I look at things. I assume people are honest. The law says they don't do it, and I assume they do not do it. If they're caught doing it, then we'll do something about it.

But I think we have come to the time where we have to assume that people obey the law. I know you might think that is a vile assumption, but I haven't found it to be so.

Senator ABOUREZK. I don't have any more questions. Thank you very much for your responses.

Senator KENNEDY. I would like to go back to the noncriminal standard and the examples which are being cited.

In this hypothetical that you gave about the canister and the CB radio and all the rest, it is difficult for me to understand.

Under the noncriminal standard that we have in the legislation, you have to show that the material is "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."

It seems to me that would be the same kind of standard as that applied in the espionage area. And if it's not, I wish you could explain why it isn't.

Mr. FUNK. Under 793 and 794, the term is national defense information. That's been interpreted by the Supreme Court broadly, but not as broadly as information which is harmful to national security.

It says: Information about our Army and Navy establishments and other matters dealing with military preparedness.

We believe that sensitive economic information which is not Government information—or classified information, for example, trade secrets—can be stolen.

Senator KENNEDY. Don't the trade secrets have to be harmful to the security of the United States?

Mr. FUNK. Or they would have to be harmful to the security of the United States, or that our failure to monitor or find out exactly what secrets were being given would be harmful.

Senator KENNEDY. Isn't that the same as espionage? If you're showing that it is going to be harmful to the security of the United States,

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

then it seems to me you should be able to get it under the espionage laws.

Mr. FUNK. It is a problem when we don't know exactly what the range of 793 and 794 are. They say national defense information. That term has been subject to some definitions by the court, and it is sufficiently unclear that we don't feel safe in assuming that this hypothetical that we gave would be under it.

Senator KENNEDY. To reach either noncriminal standard, it is going to have to be harmful to the security of the United States. Am I correct in that?

Mr. FUNK. That's correct.

Senator KENNEDY. If it is going to have to be harmful to the security of the United States—that information—I wonder why it isn't going to be enough to be able to get the warrant in terms of espionage.

Mr. FUNK. Just because that's not the term that is used in the espionage statutes. That there is national defense information which is a term of unclear purport.

Senator KENNEDY. Attorney General Bell, as a former member of the judiciary, and as one who has expressed great confidence in it, can you foresee the possibility where an espionage warrant wouldn't be granted? If you came before the judge and had shown him that the information was going to be harmful to the security of the United States? That is going to have to be the case under the noncriminal standard, and that is going to be the case in terms of espionage as well.

Is a judge really going to draw the distinction and say: Harmful to the security of the United States under this noncriminal standard is a little different from harmful to the security under espionage? If he would grant the warrant in one, he wouldn't grant it in the other?

Attorney General BELL. If you didn't have that standard there, which we have just stated, you would have to get it under the espionage statutes, which would be restricted to national defense, which is not as broad as that——

Senator KENNEDY. Harmful to the security of the United States.

Attorney General BELL. That's a much broader standard than the military security.

Senator KENNEDY. I am just not sure how a judge would react. That's what we are talking about. It seems to me that they would not grant it in one and yet grant it in the other.

Attorney General BELL. I'll tell you how the judge would react.

The criminal standard is going to be very strict. It is going to be much narrower than this.

These hypotheticals would be national security matters which would not have anything to do with defense.

The judge would say: This is a criminal statute, and I can't see that this is a probable cause for a crime. And he would deny the application.

Senator KENNEDY. Do you really think that a judge makes such a distinction when he believes that the issue is harmful to the interests and the security of the United States?

Attorney General BELL. I think he does.

Senator KENNEDY. And you're talking about a KGB agent?

Attorney General BELL. I think he would have to make a distinction if he is thinking in terms of a crime. I think that is a much more narrow standard.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Senator ABOUREZK. The espionage statute concerns information relating to the national defense. Do you make a distinction between "national security" and "national defense;" if so, what is that distinction?

Attorney General BELL. National security to me, is, for instance, industrial secrets. Suppose all the wheat in the United States was going to be bought through somebody getting information they could not otherwise get without intelligence.

And we picked that up. We know something like that is going on.

It can be all sorts of situations where the national security is involved but not necessarily the national defense.

If Congress wants us to get out of that business and just deal in national defense, then we have a much more restricted area of activity.

Senator ABOUREZK. I still don't understand what kind of a distinction you might make between "national security" and "national defense."

You related something that is economic in nature.

Attorney General BELL. Let me give you another example.

We might have somebody who is getting information about IBM computer technology, and that might be in a weapons system, but we couldn't know enough about it to convince a judge that this was a crime about to be committed and there was probable cause.

There would be a reasonable inference that could be drawn from the facts that national security was involved, but it wouldn't approach the standard of a crime.

You are dealing in so many areas of sophisticated data retrieval and computer technology. We just think it is necessary.

Senator ABOUREZK. You have talked all around this, Mr. Attorney General, but I want to get back to what kind of a distinction you draw between national defense and national security.

I don't see the distinction, and I would like to have an explanation, if you have one.

Attorney General BELL. I don't know if I can give you any more, other than say: National security to me is broader than national defense.

Senator ABOUREZK. In what respects?

Senator HATCH. Would the Senator yield for a question that might clarify this a little?

Judge Bell, in addition to certain circumstances with regard to noncriminal standards, where trade secrets and industrial processes are concerned, is it not true that activities, such as the gathering of embarrassing material about persons for possible blackmail, is not presently a Federal crime?

Senator ABOUREZK. Blackmail is a Federal crime.

Senator HATCH. That's right. Gathering materials for purposes of embarrassing and possible blackmail is not a Federal crime.

Wouldn't you agree that innocent U.S. citizens need to be protected from those types of activities as well?

Attorney General BELL. I hadn't thought about that.

Senator HATCH. But it is a good illustration, isn't it?

Attorney General BELL. Yes.

Senator ABOUREZK. Isn't blackmail a Federal crime?

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Mr. FUNK. Blackmail is a Federal crime only when you are going to disclose that a person has violated the law and you intend to get something of value in return. In other words, to reveal or disclose embarrassing information is not a Federal crime, and extortion is only illegal when interstate commerce is used.

This is one of the problems with our laws. We look at all sorts of laws that weren't written in terms of espionage that may or may not make a certain thing illegal. And we say: "Can't you get it under this or that statute?" And maybe we can under one fact situation, get them under the statute; but in another situation, we don't, because it is an area that wasn't addressed rationally and logically.

Senator KENNEDY. It is important, even when we're talking about the noncriminal standard, that the information sought would still have to fall within the foreign intelligence information definition.

If you look at the foreign intelligence definition, under the (A) section, we are talking about a potential attack, or grave and hostile acts; (B) we are taking about information which is essential to the national defense or the security of the Nation—essential in the area of foreign policy; (C) terrorism; (D) sabotage; (E) clandestine intelligence, which is basically counterintelligence. So we are not talking about "wheat" in any event.

Attorney General BELL. I was just trying to give that as an example.

I think probably the best thing to do is for us to give you an answer in writing, after we can sit down and articulate the reason for having this.

Senator HATCH. I think "wheat" is a good example, because that might very well involve national security.

Attorney General BELL. It could be, but I think we can think of a number that have nothing to do with national defense.

Senator ABOUREZK. In the last administration, Earl Butz gave them all that information when they bought the wheat in 1972.

Senator KENNEDY. Maybe there is a difference, and that is why it is important to nail this down.

To talk about wheat falling under the particular definition of foreign intelligence information as being essential to the national defense or security of the Nation ——

Attorney General BELL. If I thought somebody was going to take an economic measure against our country which was going to increase the price of a loaf of bread from 15 cents to $1, I would think it was a fairly serious matter.

That may not be a good example, but that sort of activitiy goes on among the nations now.

Senator HATCH. You used an extreme example to make your point. That there may be security matters involved that we haven't even thought of at this particular time when may be legitimate for surveillance purposes.

Attorney General BELL. That we would have to assess at the time.

We will try to write this out, since the committee is concerned about it.

We will answer in writing.

Senator KENNEDY. We had in the bill last year that you would notify the Congress concerning the application of this bill.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4
93-179 O - 77 - 4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

You have no objection to including that, so that the Congress is on notice?

Mr. BARON. In this year's bill, Senator, we did not include the full range of reporting provisions that we had in last year's bill, feeling that it was presumptuous of the executive branch to lay out what the Congress did or did not need.

Senator KENNEDY. You have no objection to provisions which would require you to report to the Congress?

Attorney General BELL. We will be glad to report it.

Senator KENNEDY. If there are no further questions, I just want to thank Attorney General Bell and Director Kelley. We will make your statement, in its entirety, a part of the record.

I'm sure we will have the good fortune and opportunity to have you before the committee again.

I want to indicate, as one member, that Director Kelley has always been very responsive to the inquiries of the members of the committee.

I want to join with those who have commented on your commendable public service in a very complex and difficult area and at a time of extraordinary difficulty for the country.

Director Kelley, we were delighted to have you here and appreciate your presence.

Senator HATCH. I would like to join in that. We appreciate both of you and the work that your are doing. I think you have done a great job under the circumstances, Director Kelley, and certainly I appreciate everything you're doing, Attorney General Bell.

Senator KENNEDY. We will recess until tomorrow morning, when we will have Mr. Turner, Director of the CIA, and Harold Brown at 9:15 a.m.

[Whereupon, at 4:00 p.m., the hearing was recessed.]

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

HEARINGS ON S. 1566 FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1977

TUESDAY, JUNE 14, 1977

U.S. SENATE,
SUBCOMMITTEE ON CRIMINAL LAWS AND PROCEDURES
OF THE COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The subcommittee met, pursuant to recess, at 9:20 a.m., in room 2228, Dirksen Senate Office Building, Senate Edward M. Kennedy, acting chairman, presiding.

Present: Senators Kennedy, Thurmond, and Hatch.

Also present: Senator Abourezk.

Staff present: Paul C. Summitt, chief counsel; D. Eric Hultman, minority counsel; Kenneth Fienberg, administrative assistant to Senator Kennedy; and Mabel A. Downey, chief clerk.

Senator KENNEDY [acting chairman]. The subcommittee will come to order.

We continue our hearings this morning on S. 1566. We had some very important and useful testimony yesterday by the Attorney General of the United States and by the head of the Federal Bureau of Investigation in support of this legislation.

We heard some very constructive responses to questions concerning some of the changes that have been made in this year's bill as compared to last year's bill. We reviewed some of the provisions that had been changed and the reasons that the administration felt those changes were necessary.

There have been some additional changes in the legislation which have been made at the request of the Secretary of Defense and the head of the Central Intelligence Agency. We look forward to examining those this morning.

We are particularly appreciative of the Director of the Central Intelligence Agency coming before this subcommittee and responding to these questions.

I have been interested in this issue for a number of years and have been a part of seven sets of hearings where it was absolutely impossible to get the Director of the Federal Bureau of Investigation not only to appear at the hearings, but to respond to some of the questions the way Mr. Kelley did yesterday.

I think it is significant that the Director of the Intelligency Agency is willing to come today and share with the American people this matter which is important to the preservation of liberty and also important to the security of the American people. It is significant that we

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

hear from the individual who the President has selected to guide the Nation in this important area. We hope to learn today, as completely and as fully as possible, the administration's policy as well as the attitude of the agency in this area of electronic surveillance. I think it is a real tribute to the concept of open government. It is the type of thing which brings great reassurance to the American people.

We are very grateful and appreciative to have both these distinguished public servants here today.

Senator Hatch, do you wish to comment?

Senator HATCH. Thank you, Mr. Chairman.

I, likewise would like to welcome both of you as well as those members of your staff who are with you.

I believe that these hearings have been very interesting thus far. There are people all over America who are concerned not only about the principles of freedom that are certainly considered by this particular legislation, and I think protected, but also the security of this Nation. What we are doing here, it seems to me, is of utmost importance to the people of this country regardless of particular philosophy or points of review.

Both Senator Kennedy and I appreciate the fact that you people would be with us here today. We are looking forward to hearing from both of you.

Senator KENNEDY. Secretary Brown, we look forward to your testimony. You may proceed.

STATEMENT OF HON. HAROLD BROWN, SECRETARY OF DEFENSE; ACCOMPANIED BY DEANNE SIEMER, GENERAL COUNSEL, DEPARTMENT OF DEFENSE

Secretary BROWN. Thank you very much, Mr. Chairman.

Mr. Chairman and members of the committee, I appear before you today at your invitation to testify with respect to S. 1566, the proposed Foreign Intelligence Surveillance Act.

Various agencies of the Department of Defense have an important role in the collection and analysis of foreign intelligence of all kinds. Our intelligence activities provide information about foreign military capabilities, the intentions of foreign powers, and other activities of foreign governments as well. These various sorts of intelligence often are inextricably intertwined.

A single channel of communication under surveillance may yield information on subjects ranging from troop deployments and morale to grain harvests. A single bit of intelligence—such as information that a division of an Eastern European army is advancing to a border area—can be vitally important not only to the U.S. military commander on the other side of that border, but also the President, the Secretary of State, the Director of Central Intelligence, and the Secretary of Defense.

From the point of view of the Department of Defense, adequate and dependable surveillance for military defense and planning is essential, and therefore the legislation you are considering today is important to me.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Agencies of the Department having an important role in the foreign intelligence collection effort are: The Army Assistant Chief of Staff for Intelligence; the Director of Naval Intelligence; the Air Force Assistant Chief of Staff for Intelligence; the Deputy Assistant Secretary of Defense for Administration, who handles military counterintelligence; the Defense Intelligence Agency; and the National Security Agency.

All work closely together. Each has both general responsibilities and a specialized mission which is coordinated with the activities of other entities in the intelligence community by the Director of Central Intelligence.

Since coming into office I have personally taken action to tighten the controls on approval of electronic surveillance and to assure that each of the DOD intelligence entities operates within the requirements for electronic surveillance set out pursuant to Executive Order 11905. One of my first actions on assuming office was to establish a special committee to make recommendations for improvements in the way intelligence activities are handled within the Department.

Moreover, on February 8, 1977, I issued a memorandum which states my position clearly. I have a copy here and can make it available for the record.

It says, "I will not condone Defense intelligence activities which violate or infringe on the constitutional rights of U.S. citizens. In this connection, I expect that all intelligence and counterintelligence functions carried out by your department or agency are strictly within the law."

I believe the committee actually has a copy of this already.

In February I met with the Directors of the National Security Agency and the Defense Intelligence Agency and in the Armed Forces Policy Council I met with Secretaries of the Army, Navy, and Air Force and the Joint Chiefs of Staff to emphasize personally to them my commitment that tighter controls be applied.

The operations of most of the intelligence components of the Defense Department are carried out overseas.

Upon a review of our records, it has been determined that the Attorney General has only approved one of the six new electronic surveillance requests made since the new administration came into office. The Inter-Agency Review Panel has forwarded three others to him but he has taken no action as yet. The Panel sent one request to the intelligence community staff for further justification; in addition, the Panel decided not to forward one request to the Attorney General.

Senator KENNEDY. Were those American citizens?

Secretary BROWN. No.

This bill does not apply to surveillance activities conducted outside the United States.

Senator KENNEDY. Can you tell me how many that you actually received were approved?

Secretary BROWN. One was not approved.

Senator KENNEDY. Who disapproved it?

Secretary BROWN. That was disapproved at an NSC interagency panel.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Again, I want to emphasize that none of those had to do with U.S. citizens. In fact, they did not have to do with individuals at all.

Senator KENNEDY. I think that is important. It was not individuals.

Secretary BROWN. It was foreign powers.

The bill that you are considering today does not apply——

Senator KENNEDY. Let me just ask one more question. Had they been going on before? Were they continued taps or new initiatives?

Secretary BROWN. These were new ones.

This bill that you are considering today does not apply to surveillance activities conducted outside the United States. The relevant legal requirements for those activities will be set out in an overseas counterpart to the bill you are considering today. Of course, we consider that an extremely important matter and worthy of prompt attention.

The President has given you his assurance that the administration will support an appropriate bill regulating overseas electronic surveillance activities, and the effort to draft such a bill is underway.

I think it is important that the regulation of domestic and foreign electronic surveillance for intelligence purposes be kept separate. The operations are different, the problems are different, and the impact of legal restrictions on the intelligence-gathering effort is different. Trying to accommodate all of these differences in one law inevitably makes the law more difficult to administer.

The intelligence agencies need clear mandates and guidelines, and a separation of the legal requirements for domestic operations and foreign operations will best accomplish that end.

Senator KENNEDY. Could you elaborate on that, Mr. Secretary. Why is that so important?

Secretary BROWN. I think, Mr. Chairman, that in the United States one is sometimes dealing, even if inadvertently, with U.S. citizens. Overseas there is a separate set of issues.

Although I would argue that actions of U.S. officials need to be governed by U.S. laws wherever they are, it seems to me questionable whether the same kinds of protections are applicable to foreign powers overseas as they are to U.S. citizens, for example, in the United States.

Senator KENNEDY. What about U.S. citizens overseas? That is a troublesome problem. It is of interest to Senator Bayh and other members of the committee.

Secretary BROWN. U.S. citizens overseas present, again, a somewhat different problem. I find it difficult to go into more detail in open session.

Senator KENNEDY. What kinds of protection ought to be made available to people overseas? Should you have a warrant or not?

That is not the purpose of this legislation so I want to move through it quickly.

Secretary BROWN. I would want to think about it. I believe that U.S. citizens overseas are entitled to protection.

I think, Mr. Chairman, that the most important accomplishment of S.1566, the proposed legislation you have before you, is the creation of a uniform system of accountability for all of the agencies and components of the intelligence community with respect to electronic surveillance conducted within the United States.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

The collection of foreign intelligence through electronic surveillance, like other aspects of our foreign intelligence activities, benefits from a diversity of approaches and the participation of a number of different government entities with different needs and expert resources.

A uniform system of accountability permits us to continue to reap the benefits of this diversity of approaches and at the same time accomplish our goal of restoring public confidence that our foreign intelligence capability will not be diverted to improper purposes.

In my view, Mr. Chairman, that goal of restoring public confidence is a central one. If we are to be able to do our job with respect to foreign intelligence, the American people and the American Congress must believe, and that belief must be based on the facts, that the agencies of Government are not using our foreign intelligence capability improperly.

I view this bill as requiring the active participation of the chiefs of each of the intelligence activities within the Department of Defense. I view the certification requirements as mandating my personal attention to and decision about the appropriateness of a request for a warrant to conduct electronic surveillance within the United States.

If the bill is enacted in its present form and I am designated by the President as a certifying authority, I would plan to establish four general procedures for carrying out my responsibilities.

First, I would limit the authority to make application for a warrant to the chiefs of the intelligence activities within the Department of Defense. This would mean that each application for a warrant would be backed by the personal oath or affirmation of one of the six senior officials who has operating responsibility for foreign intelligence collection activities within my supervision. I would probably have to make some provision for emergencies and absences, but it would be my intention to require the personal attention and undertaking of my most senior intelligence aides in this regard.

Second, I would require the preparation of detailed backup information to be presented either in written form or orally. This backup material would address each of the five items required by the bill:

First, the identity of the target and the basis for the necessary determinations we have to make about the target, including whether the target is a U.S. person;

Second, the type of information we can expect to obtain from electronic surveillance of the target and the basis for the necessary determinations we have to make about that information, including whether the information is foreign intelligence;

Third, the type of electronic surveillance we will have to use to get the information and the basis for the necessary determinations about these means, including whether the information can be obtained by normal investigative techniques not requiring electronic surveillance;

Fourth, the period of time for which we would have to use electronic surveillance to get the information we are seeking; and

Fifth, the type of minimization procedures we will have to use to ensure that information concerning U.S. persons is not acquired, retained, or disseminated unless it is foreign intelligence.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Not all of this information would be required to be set out in the application, but I would require it to be prepared in each case so that I am assured that each of the statutory requirements has been met. The Attorney General could, of course, be provided this backup information if he needed it.

The third general procedure that I would establish for carrying out my responsibilities is that I would require the application and backup information to be reviewed by the General Counsel of the Department of Defense, who happens to be Miss Siemer sitting on my right, so that we would have an independent legal judgment as to the sufficiency of the basis for the certification and the statements required to be made in the application.

Fourth, I would personally review the application and would personally make the required certification subject only to contingency arrangements to take care of requirements which may arise in my absence.

That procedure would impose a substantial burden on me and on the Department of Defense, but I think the end result will be a workable system that will provide the necessary accountability for all intelligence activities conducted by the Department.

That procedure would also create substantial needs for protection of foreign intelligence sources and methods and I want to emphasize how important it is that the bill also be adequate in these regards.

We will be generating documents that contain some of our most valuable intelligence secrets: for example, the identity of the targets of our intelligence-gathering activities; the type of information we expect to get from those targets; and the means we use to get that information.

These documents will pass out of the control of the intelligence community and into the judicial system. They will become the subject of intense discovery efforts both by clandestine means, through the efforts of intelligence services of other governments, and by normal litigation means, through the efforts of lawyers representing clients whose communications may have been acquired.

Senator KENNEDY. Mr. Secretary, I have gone through your prepared statement. You have outlined the procedures which will be followed, and I think it will be very useful, but in the interest of time could we include your entire statement in the record. Then Admiral Turner can summarize his statement. Then we can get into some of the particular changes and some of the particular questions. Is that an agreeable way of proceeding?

Secretary BROWN. Fine.

[Material follows:]

STATEMENT OF HAROLD BROWN, SECRETARY OF DEFENSE

Mr. Chairman and members of the committee, I appear before you today at your invitation to testify with respect to S. 1566, the proposed Foreign Intelligence Surveillance Act.

Various agencies of the Department of Defense have an important role in the collection and analysis of foreign intelligence of all kinds. Our intelligence activities provide information about foreign military capabilities, the intentions of foreign powers, and other activities of foreign governments as well. These various sorts of intelligence often are inextricably intertwined. A single channel

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

of communication under surveillance may yield information on subjects ranging from troop deployments and morale to grain harvests. A single bit of intelligence—such as information that a division of an Eastern European army is advancing to a border area—can be vitally important not only to the United States military commander on the other side of that border, but also the President, the Secretary of State, the Director of Central Intelligence, and the Secretary of Defense. From the point of view of the Department of Defense, adequate and dependable surveillance for military defense and planning is essential, and therefore the legislation you are considering today is important to me.

Agencies of the Department having an important role in the foreign intelligence collection effort are:

The Army Assistant Chief of Staff for Intelligence;
The Director of Naval Intelligence;
The Air Force Assistant Chief of Staff for Intelligence;
The Deputy Assistant Secretary of Defense for Administration (who handles military counterintelligence);
The Defense Intelligence Agency; and
The National Security Agency.

All work closely together. Each has both general responsibilities and a specialized mission which is coordinated with the activities of other entities in the Intelligence Community by the Director of Central Intelligence.

Since coming into office I have personally taken action to tighten the controls on approval of electronic surveillance and to assure that each of the DOD intelligence entities operates within the requirements for electronic surveillance set out pursuant to Executive Order 11905. One of my first actions on assuming office was to establish a special committee to make recommendations for improvements in the way intelligence activities are handled within the Department. On February 8, 1977, I issued a memorandum which states my position clearly. It says:

"I will not condone Defense intelligence activities which violate or infringe on the constitutional rights of United States Citizens. In this connection I expect that all intelligence and counter-intelligence functions carried out by your department or agency are strictly within the law."

A copy has been supplied to the Committee. I also met in February with the Directors of the National Security Agency and the Defense Intelligence Agency and with the Joint Chiefs of Staff to emphasize personally to them my commitment that tighter controls be applied.

The operations of most of the intelligence components of the Defense Department are carried out overseas. Since I became Secretary of Defense, the Department of Defense requested approval from the Attorney General for new electronic surveillance within the United States on only six occasions. This bill does not apply to surveillance activities conducted outside the United States. The relevant legal requirements for those activities will be set out in an overseas counterpart to the Bill you are considering today. The Persident has given you his assurance that the Administration will support an appropriate bill regulating overseas electronic surveillance activities and the effort to draft such a bill is underway. I think it is important that the regulation of domestic and foreign electronic surveillance for intelligence purposes be kept separate. The operations are different, the problems are different, and the impact of legal restrictions on the intelligence-gathering effort are different. Trying to accommodate all of these differences in one law inevitably makes the law more difficult. The intelligence agencies need clear mandates and guidelines, and a separation of the legal requirements for domestic operations and foreign operations will best accomplish that end.

In my view, the most important accomplishment of S. 1566, the proposed legislation you have before you, is the creation of a uniform system of accountability for all of the agencies and components of the Intelligence Community with respect to electronic surveillance conducted within the United States. The collection of foreign intelligence through electronic surveillance, like other aspects of our foreign intelligence activities, benefits from a diversity of approaches and the participation of a number of different government entities with different needs and expert resources. A uniform system of accountability permits us to

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

continue to reap the benefits of this diversity of approaches and at the same time accomplish our goal of restoring public confidence that our foreign intelligence capability will not be diverted to improper purposes.

I view this bill as requiring the active participation of the chiefs of each of the intelligence activities within the Department of Defense. I view the certification requirements as mandating my personal attention to and decision about the appropriateness of a request for a warrant to conduct electronic surveillance within the United States.

If the Bill were enacted in its present form and I were designated by the President as a certifying authority, I would establish four general procedures for carrying out my responsibilities.

First, I would limit the authority to make application for a warrant to the chiefs of the intelligence activities within the Department of Defense. This would mean that each applicant for a warrant would be backed by the personal oath or affirmation of one of the six senior officials who has operating responsibility for foreign intelligence collection activities within the Department. I would probably have to make some provisions for emergencies and absences, but it would be my intention to require the personal attention and undertaking of my most senior intelligence aides in this regard.

Second, I would require the preparation of detailed backup information to be presented either in written form or orally. This backup material woud address each of the five items required by the Bill:

(1) The identity of the target and the basis for the necessary determinations we have to make about the target including whether the target is a United States person;

(2) The type of information we can expect to obtain from electronic surveillance of the target and the basis for the necessary determinations we have to make about that information including whether the information is foreign intelligence;

(3) The type of electronic surveillance we will have to use to get the information and the basis for the necessary determinations about these means, including whether the information can be obtained by normal investigative techniques not requiring electronic surveillance;

(4) The period of time for which we would have to use electronic surveillance to get the information we are seeking; and

(5) The type of minimization procedures we will have to use to ensure that information concerning United States persons is not acquired, retained, or disseminated unless it is foreign intelligence.

Not all of this information would be required to be set out in the application, but I would require it to be prepared in each case so that I am assured that each of the statutory requirements has been met. The Attorney General could, of course, be provided this backup information if he need it.

Third, I would require the application and backup information to be reviewed by the General Counsel of the Department of Defense so that we would have an independent legal judgment as to the sufficiency of the basis for the certification and the statements required to be made in the application.

Fourth, I would personally review the application and would personally make the required certification subject only to contingency arrangements to take care of in my absence.

That procedure would impose a sustantial burden on me and on the Department of Defense, but I think the end result will be a workable system that will provide the necessary accountability for all intelligence activities conducted by the Department.

That procedure would also create substantial needs for protection of foreign intelligence sources and methods and I want to emphasize how important it is that the Bill also be adequate in these regards. We will be generating documents that contain some of our most valuable intelligence secrets:

The identity of the targets of our intelligence gathering activities;
The type of information we expect to get from those targets; and
The means we use to get that information.

These documents will pass out of the control of the Intelligence Community and into the judicial system. They will become the subject of intense discovery efforts both by clandestine means, through the efforts of intelligence services of other governments, and by normal litigation means, through the efforts of lawyers representing clients whose communications may have been acquired.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Several of the provisions of the Bill are important in protecting the security of this information and I hope any changes made to these provisions during the legislative process expand these protections.

First, Section 2523(c) provides for security measures to protect the applications for warrants, the orders granting or denying warrants, and the records of the warrant proceedings. This should remain flexible so that if no satisfactory arrangement can be worked out using existing court procedures and facilities, authority and funds necessary will be available to create alternatives. The most skilled foreign intelligence agents in the world will be seeking this information and we should not be hindered in our efforts to keep it from them.

Second, Section 2524(c) and Section 2525(c) provide that a judge may require an application to be supplemented by such other information (other than the application and the certification) as is necessary to make the determinations or findings mandated by the statute. It is important that the qualifying term "necessary" remain an integral part of this provision and that it be made clear that the term "necessary" when used in this context means substantially more than just "useful" or "helpful." The statute is designed so that, if properly implemented, the application and certification provide all the information necessary to these findings and determinations. Only in an unusual case should a judge need more.

Third, Section 2526(a) provides that information obtained from foreign intelligence electronic surveillance may be used for law enforcement purposes only if its use outweighs the possible harm to the national security. This gives the Attorney General explicit authority to decline to prosecute where to do so would entail a risk of exposure of intelligence information. Since these determinations are, of necessity, made within the Executive Branch and without explanation, it is important that there be an acknowledgment that the Congress intended this balancing process to take place. This provision will also deter judicial interpretations of this bill in the future to create any right to disclosure of national security information.

Fourth, Section 2526(c) provides for limited disclosure in litigation. If a motion is made to discover or suppress evidence on grounds that it was obtained from an unlawful electronic surveillance the statute authorizes disclosure to the judge in that proceeding, for an in camera review, and authorizes disclosure to the aggrieved person in special circumstances. There are two important limitations that, in my view, are essential. The only information that may be disclosed to either the judge or the aggrieved person is the application, the order, and relevant portions of the transcript of the surveillance.

This limitation is necessary to protect against an expansive interpretation of the Bill in the future that would permit access to any backup documents that may exist. Further, the application, order and transcript may be disclosed to the judge only to the extent necessary to make a determination as to whether the electronic surveillance was lawful, and may be disclosed to an aggrieved person only to the extent that this person's participation is necessary to make that determination. Here again, the qualifier "necessary" is extremely important and must be intended to mean substantially more than "useful" or "helpful."

In conclusion, Mr. Chairman, I would point out that the Bill before you protects the rights of Americans not only to the extent that they are required to be protected by the courts' interpretations of the Fourth Amendment, but beyond that to the extent they are required to be protected to meet the reasonable expectations of our people. The Bill also protects our valuable foreign intelligence sources and information from unnecessary disclosure which weakens our national security. The accommodation of both these important national interests requires provisions that might appear less than ideal if considered from only one of the various points of view that are involved. I am satisfied with this Bill which has been worked out over several months of effort by your staffs and mine. I hope the members of the Committee will find it satisfactory as well.

Thank you.

Senator KENNEDY. Mr. Turner, you may proceed.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

STATEMENT OF ADM. STANSFIELD TURNER, DIRECTOR OF CENTRAL INTELLIGENCE; ACCOMPANIED BY ANTHONY A. LAPHAM, GENERAL COUNSEL, CENTRAL INTELLIGENCE AGENCY; AND REAR ADM. D. M. SHOWERS, U.S. NAVY (RETIRED), INTELLIGENCE COMMUNITY STAFF

Admiral TURNER. Let me summarize my statement very, very briefly, Mr. Chairman.

I support this legislation looking at it from two points of view—one, protecting the rights of the citizens of our country and, two, ensuring that we have the needed opportunity to collect foreign intelligence in the interest of our country's security and welfare.

Clearly this bill will inhibit the collection of foreign intelligence to some degree. However, in my view that is worth the increase in credibility and the increased assurance of the people of the United States in their intelligence operations and in the protection of their rights.

I think it strikes a proper compromise between these two somewhat conflicting requirements. I believe we can satisfactorily meet the intelligence needs of the country under the provisions of this bill.

Senator KENNEDY. Your prepared statement in its entirety will be made a part of the hearing record.

[Material follows:]

STATEMENT OF ADMIRAL STANSFIELD TURNER, DIRECTOR OF CENTRAL INTELLIGENCE

Mr. Chairman, thank you, Mr. Chairman and members of this subcommittee, for your invitation to appear and express my views on S. 1566, the proposed legislation which deals with electronic surveillance undertaken in the United States to obtain foreign intelligence. I have a brief statement that I would like to present and I will then by happy to expand on any particular aspect of my statement or to respond to any other question which may be of interest to the subcommittee.

I support the proposed legislation. I support it because I believe it strikes a fair balance between intelligence needs and privacy interests, both of which are critically important. I support it as well because I believe it will place the activities with which it deals on a solid and reliable legal footing, and thus hopefully bring an end to the uncertainty about the limits of legitimate authority with respect to these activities, and about how, by whom, and under what circumstances that authority can rightfully be exercised. I favor the proposed legislation for additional reasons, not the least of which is my view that its enactment will help to rebuild public confidence in the national intelligence collection effort and in the agencies of Government principally engaged in that effort.

Electronic surveillance is of course an intrusive technique, involving as it does the interception of non-public communications. At the same time it is a necessary technique, and in my opinion a proper one, so far as concerns the gathering of foreign intelligence and counterintelligence within the United States. The fundamental issue therefore, as I see it, is how to regulate the use of electronic surveillance so as to safeguard against abuse and over-reaching without crippling the ability to acquire information that is vital to the formulation and conduct of foreign policy and to the national defense and the protection of the national security. In part that is a legal issue. In larger part, however, the question is political.

As matters now stand, electronic surveillance in the field of foreign intelligence is carried out without judicial warrant, under a written delegation of authority from the President and pursuant to procedures issued by the Attorney General. Under the delegation and the procedures, all surveillance requests must be submitted to the Attorney General. No surveillance may be undertaken without the prior approval of the Attorney General, or the Acting Attorney General, based on his determination that the request satisfies specific criteria relating to the quality of the information sought to be obtained, the means of acquisition, and the character of the target as a foreign power or agent of a foreign power. These

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

criteria closely resemble the standards that would apply, by force of statute, were the proposed legislation to be enacted. Indeed, to the extent I have knowledge of these matters, I am not aware of any electronic surveillance now being conducted for foreign intelligence purposes under circumstances that would not justify the issuance of a judicial warrant were S. 1566 to become law, barring any significant amendments.

I am advised that the present practices conform to all applicable legal requirements, including the requirements of the Fourth Amendment. However, assuming as I do that the President has the constitutional power to authorize warrantless electronic surveillance to gather foreign intelligence, it must still be answered whether the present arrangements, under which the approval authority is reserved to the executive branch, represent the wisest public policy given the privacy values that are at stake and given the potential for the subversion of those values.

The proposed legislation reflects a conclusion that the existing arrangements do not represent the wisest policy and that the power to approve national security electronic surveillance within the United States should be shared with the courts. I accept that conclusion, as does the President, and I accept as well the warrant requirement that is the central feature of the bill. As the Director of Central Intelligence, of course, I am necessarily concerned about the capacity of the U.S. intelligence establishment to collect and provide a flow of accurate and timely foreign intelligence information, and I have a responsibility to prevent the unauthorized disclosure of the sources of that information and the methods by which it is obtained. I have therefore tried to assess what the enactment of S. 1566 might cost in terms of lost intelligence or reduced security. Based on my careful review of the bill, I cannot say to you flatly that there will not be such costs.

It is possible, for example, that the bill's definitions of foreign intelligence information will prove to be too narrow, or will be too narrowly construed, to permit the acquisition of genuinely significant communications. It is likewise possible that justified warrant applications will be denied, or that the application papers will be mishandled and compromised. These possibilities are difficult to measure, but they are risks. In the end, however, I think they are risks worth taking. The fact of the matter is that we are already paying a price, equally difficult to measure but nonetheless real, in terms of public suspicions and perceptions that surround the present arrangements. A release from these burdens of mistrust is itself a consideration that argues in favor of the bill. In addition, as I read the bill, specifically sections 2523(c) and 2525(b), the Director of Central Intelligence will have a role in determining the security procedures that will apply to the warrant application papers and the records of any resulting surveillance, and that is a responsibility to which I intend to devote serious attention.

As the subcommittee knows, much of the information that is likely to be obtained from electronic surveillance covered by this bill will not relate, even incidentally, to U.S. persons, with whose privacy rights the bill is specially concerned. Even so, an assurance that all such activity within the United States is conducted lawfully, under rigid controls, and with full accountability for the action taken, whether or not it impinges in any way on the communications of U.S. persons, would be a major step forward, and in my estimation this bill will provide that assurance.

In sum, I regard the preposed legislation as desirable and urge its early consideration and adoption.

Senator KENNEDY. Those are very important words coming from the head of the Intelligence Agency, words about the protection of the civil liberties of the American people.

Every one of us is very much aware of the important responsibilities which you have in terms of protecting the security interests of this country. From your statement you obviously understand that this is an important balance. That is extremely reassuring. Your statements, your comments, and your support for the legislation are reassuring.

Secretary Brown, I would like to review briefly with you some of the changes in the legislation made in the area of "use of information." That is on page 21 of the new bill and page 25 of the old bill.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

In the new bill we have added, I understand at your request, "information concerning United States persons acquired from electronic surveillance."

You mention, "only for the purpose specified in section 2521," et cetera, "or for the enforcement of the criminal law if its use outweights the possible harm of the national security."

I am just wondering why that language is necessary. It seems to me that was understood in the old legislation. It is basically an executive determination. We are very much aware of that precedent. That has generally been the way executive branch determinations have been made over the period of the past.

I am wondering what real value or use it is to add that. I personally do not think that it adds anything. Maybe we are just raising a flag here which is unnecessary and which may, under rather convoluted reasoning, be a misconstruction.

Would you comment on that?

Secretary BROWN. Yes, Mr. Chairman.

As I indicated in my statement, I think it is desirable to give the Attorney General explicit authority to decline to prosecute where doing so would entail a risk of exposure of intelligence information. I think that is a balance that has to be drawn.

Since those decisions will be made within the executive branch without explanation, I think it is important to have in the law an indication that the Congress intends to have a balancing process.

Also, I would point out that in some ways that can be considered a way of preventing abuses. I think that information obtained for foreign intelligence purposes and then used for criminal proceedings, particularly if it is obtained against people not targeted, does raise a question of abuse.

Senator KENNEDY. Of course the Attorney General has not really requested it. He does not really desire it. I am wondering why, if he does not feel that it is necessary in establishing that balance, we ought to have it.

How upset would you be if we did not include that?

Secretary BROWN. I would be concerned because the disclosure of the information could, I think, in many cases really hurt U.S. intelligence-gathering techniques and it could hurt U.S. national security.

Senator KENNEDY. Of course we understand that. That is true today. It has always been true in terms of prosecution, whether the Department is going to move ahead in terms of prosecution and identify a particular target and, perhaps, be forced to expose other important intelligence-gathering resources. That exists today. Those choices and alternatives are constantly being made within the administration today.

I think that is understood. It is a prosecutorial decision made within the executive branch in consultation with other agencies.

I am wondering whether your language really adds very much. I understand your sensitivity and I think all of us are sensitive to that. Hopefully and decision that is going to be made will be made in the national interest, whether it is in terms of carrying forward a prosecu-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

tion or not doing it. The people who have that information obviously are going to have to make the judgments.

Why we need that decision identified as such I do not understand. It just seems to me to be unnecessary.

Secretary BROWN. I think, Mr. Chairman—and this is indeed a matter of judgment—that it would be wise to make explicit national security as a basis for balancing such considerations in a decision not to prosecute. Otherwise I have some concern that, in fact, national security interests will not be adequately considered or that judicial interpretations of the bill in the future could compel disclosure or create a right to disclosure of national security information.

It is not just going to be information for the Defense Department but for the intelligence community as a whole. Therefore, perhaps the Director of Central Intelligence would want to comment.

Admiral TURNER. Mr. Chairman, I would like to say that almost every day I am confronted with this issue of can we release some information. It is frequently for judicial purposes.

While this provision in the law would not change that procedure—we would still protect the national interest—this would give the legislative branch support for that.

I am criticized every day for being unwilling to release things when I have to make these tough decisions. It would be a help to me to have the endorsement of the legislative branch that that is a legitimate requirement.

Senator KENNEDY. You would not mind, then, if the legislative branch makes a different decision.

[Laughter.]

Senator KENNEDY. I understand what your point is. It seems to me those are tough and difficult decisions. No one is questioning that.

Mr. Turner, regarding the testing of electronic equipment used for counterintelligence purposes, under the old bill we had the 90-day provision with the approval of the Attorney General. Under the the new bill there is no 90-day provision for counterintelligence.

That is on page 27.

Could you indicate to us reasons why that 90-day limit should not be included. Do you have any strong feelings about that?

Admiral TURNER. We can live with the 90-day limit, Mr. Chairman. The added flexibility under the present system has its desirability.

Senator KENNEDY. Mr. Secretary, to your knowledge is the U.S. Army or any armed service branch engaged in any electronic surveillance of American citizens?

Secretary BROWN. None of the Department of Defense components engages in intelligence wiretapping in the United States. The Justice Department handles those based on the intelligence community needs.

We do engage in consensual wiretapping for criminal investigation or law enforcement purposes within the United States. Consensual wiretapping does not require ——

Senator KENNEDY. Could you tell us a little more about that.

Secretary BROWN. One party to the conversation agrees to have the conversation ——

Senator KENNEDY. But this is in the area of criminal investigations?

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Secretary BROWN. That is right. It is not intelligence matters. These are criminal matters concerning individual members of the armed forces, for example, engaged in criminal activities or suspected of criminal activities on U.S. Government reservations.

Senator KENNEDY. Doesn't the Attorney General sign those?

Secretary BROWN. Not if they are consensual. In other words, not if the person whose telephone is being listened to gives approval for that. While consensual wiretapping activities do not require the approval of the Attorney General, he or his designee must approve consensual non-telephonic surveillance conducted for investigative purposes within the United States. This requirement was established in 1972 by Attorney General Kleindienst and applies to all Federal departments and agencies.

Senator KENNEDY. That is the total——

Secretary BROWN. That is the total of our wiretapping activities, the ones in which we engage.

Senator KENNEDY. What is the role of the army?

Secretary BROWN. That includes all of the Defense Department agencies, all of the Services and all of the investigative agencies of the Defense Department.

Senator KENNEDY. There is no foreign intelligence gathered by the army; is that correct?

Secretary BROWN. Not in the United States. There is no intelligence wiretapping in the United States.

Senator KENNEDY. What about wiretapping by the army of American citizens overseas?

Secretary BROWN. Those are handled, to the very limited extent that they take place, through the Attorney General. We would get the Attorney General's approval. There is an elaborate procedure for that.

Senator KENNEDY. Every time the Army is involved in a wiretap overseas?

Secretary BROWN. There is an elaborate procedure in Executive Order 11905 through which we get the Attorney General's approval.

Again, the case I mentioned before was an exception where the individual involved gives his consent. In that case we do not go through those procedures.

Senator KENNEDY. The types of cases that you mentioned before, the six different foreign powers—what types of cases are those?

Secretary BROWN. I do not think I would want to discuss that in open session, Mr. Chairman.

Senator KENNEDY. Can you tell us to the extent it is counterespionage.

Secretary BROWN. It is foreign intelligence in every case. Counterintelligence is one kind of foreign intelligence.

Senator KENNEDY. Do you ever ask the FBI to conduct wiretapping for you?

Secretary BROWN. We make requests to the Justice Department. The FBI is an arm of the Justice Department in that role.

Senator KENNEDY. Can you tell us which type of wiretapping they do?

Secretary BROWN. In the United States when one of the military departments identifies a target for counterintelligence monitoring, we ask the FBI to assume jurisdiction over the investigation.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

For example, this might be a military person suspected of being engaged in espionage or otherwise acting as an agent for a foreign power.

Again, in those cases we ask the FBI to assume jurisdiction over the investigations.

Senator KENNEDY. Mr. Turner, how do you go about protecting American citizens from foreign intelligence surveillance conducted by foreign powers? There are, obviously, efforts by foreign powers to electronically survey American citizens, is there not?

Admiral TURNER. Yes, sir.

Senator KENNEDY. Can you describe what efforts you make or what steps you take to try to protect American citizens in this area?

Admiral TURNER. It is part of our overall counterintelligence program to do everything we can to find out what foreign powers are doing against our intelligence apparatus and against our citizenry. We have numerous technical means of detecting such activity. When we do locate them, it is our effort to find every way we reasonably can to counter that, to prevent it from happening.

We are into a very delicate field and treading on classified sources here, Mr. Chairman. At the same time we are into a very technical field.

Senator KENNEDY. Just in general terms, how widespread is the foreign power surveillance of American citizens? I think American citizens are entitled to know. Is it continuing? Is it ongoing? How pervasive is it?

We heard from the FBI yesterday that there are no American citizens who are being tapped by our Government for foreign intelligence purposes.

What kind of threat is there to American citizens from foreign intelligence efforts by other foreign powers? How widespread is it? Is it growing? What can you tell us about it in general terms?

Admiral TURNER. I have no indication of any alarming rate of growth. We are not confident we know all that is going on. We are trying to keep track of it as best we can.

I do not think at this stage it constitutes a serious invasion of the individual's privacy. I think such targeting as takes place is more against organizational and governmental bodies than it is against individual citizens of the country because the return in terms of the kind of information foreign powers seek against us is greater in those fields.

Senator KENNEDY. How would you assess the efforts of the Intelligence Agency in counteracting foreign efforts? I am sure you are going to say, "We are never satisfied and we are trying to do better." However, can you give us a little more of a sense as to how effective our counterintelligence efforts have been in neutralizing that?

Admiral TURNER. In a very general sense, moderately successful, Mr. Chairman. There are immense technical as well as legal impediments to stopping this kind of thing entirely.

Senator KENNEDY. In the area of the noncriminal standard, with which you are familiar, how important is it that that be continued?

We went through some verbal gymnastics yesterday in trying to realize how important or essential it is. Very frankly, we continue to be troubled by the answers we have been getting.

93-179 O - 77 - 5
Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

I am just wondering, Secretary Brown, whether you have any views. Can you help us by giving us some hypotheticals which could possibly justify that particular standard?

Secretary BROWN. Mr. Chairman, I have looked over the background of the issue and find it a complex one. It is primarily a counterintelligence problem—requiring a noncriminal standard for electronic surveillance.

The Defense Department does some military counterintelligence activities that would be affected or might be affected by such a provision. However, the noncriminal standard is principally an FBI requirement rather than a DOD requirement.

Senator KENNEDY. I beg your pardon.

Secretary BROWN. The noncriminal standard question is principally one on which the FBI would have to comment because they are the ones who deal mostly with the counterintelligence.

Senator KENNEDY. Most of the examples they give involve various groups such as Americans who may be cooperating with the KGB and stealing IBM's secrets. Most of the examples were not very good ones, quite frankly.

However, we did get important assurances that the intention is to revise the espionage laws and that those provisions would not be necessary with a recodification of the espionage laws.

Secretary BROWN. In the United States, Mr. Chairman, we do not target persons; we target the governments of foreign powers. Therefore, I do not think that provision or that question arises. I am now talking about the Department of Defense.

Under those circumstances I think anything I could offer would be an opinion for which I have no responsibility. Therefore, I would prefer not to offer an opinion.

Senator KENNEDY. Admiral Turner, do you wish to comment?

Admiral TURNER. I would like to return to your previous question, Mr. Chairman.

There are cases in which we are very confident foreign powers are attempting to intercept communications inside this country. Hypothetically we could find an American person who is aiding and abetting that process. With the means we have technically of detecting this interception going on, I am not clear in all cases that we could make a criminal case out of it. It is a criminal act. There is no question about that. Whether I could adduce sufficient evidence for the Government to press a criminal case in some instances because of the technical means involved is questionable.

Therefore, I can construct a very hypothetical instance where we would not be able to proceed unless we had a provision with noncriminal applicability.

Senator KENNEDY. Would you be satisfied if it were focused more in the direction of foreign powers? I am talking about the noncriminal standard?

Maybe we can reach your concern that way. We can go back to the FBI in terms of their particular concern. Would this meet your interests?

Admiral TURNER. Yes, sir, it would. That is my understanding of the way it is worded.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Senator KENNEDY. Admiral Turner, what types of cases are you interested in with regard to surveillance under this bill? Is it all counterintelligence?

Admiral TURNER. No, sir. It is equally or more on foreign intelligence itself.

Senator KENNEDY. Can you give us some idea of the balance we are talking about here? Would you elaborate on what percent and the types?

Admiral TURNER. My guess would be that it is predominantly for the purposes of collecting foreign intelligence, collecting information that will assist us in establishing our political, our military, and our economic policies and assist us in understanding the activities of foreign powers in all three of those fields.

Senator KENNEDY. Does the FBI do this for you?

Admiral TURNER. Yes, sir. The Central Intelligence Agency is specifically prohibited from participating in this activity.

Senator KENNEDY. I will come back to some questions about how that relationship works between you and the FBI. Maybe you could just briefly comment about how that relationship works. Do you just call them up and ask them to wire tap?

Admiral TURNER. No, sir. Today there is a very elaborate, thorough review procedure. If one of the intelligence agencies, any one, wants to have wiretapping or electronic surveillance conducted in the United States, it makes appropriate application with extensive justification. This is reviewed by what we call an interagency review panel on which the State Department, the intelligence community, the Central Intelligence Agency, the Department of Justice, and the Department of Defense are represented.

That panel reviews these very carefully. It has never in the time I have been in this office approved all of the applications that were considered at any given time.

Those are then sent to the Assistant to the President for National Security Affairs and forwarded to the Attorney General, who then in turn transmits specific action requests to the Federal Bureau of Investigation.

I think that citizen rights are well protected here by this multidepartmental review process.

These are reviewed every 90 days to make sure they are still warranted.

Senator KENNEDY. Senator Hatch?

Senator HATCH. Thank you, Mr. Chairman.

Section 2526(a), on which Senator Kennedy has raised questions, appears to me to be an important provision for protecting information gathered from foreign intelligence surveillance within the United States and within the legitimate national security concern.

How important do you consider that language to be? That is in section 2526(a).

Admiral TURNER. I consider it very helpful to us to have this provision in here as to the importance of weighing the national interest versus the criminal prosecution. I mentioned previously that we are very suspect for withholding information from the criminal procedures in the country, but that is a responsibility which we have to as-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

sume. We try our best to be as liberal as we can in interpreting what will harm the national interest.

It would be a help to have this specific provision in here in support of the times when we have to decline to release information for criminal proceedings.

Senator HATCH. It would be helpful from the standpoint of legitimate national security concerns?

Admiral TURNER. Yes.

Senator HATCH. I asked this yesterday. As you will recall, this bill provides for seven district judges to become the approving panel or to be the approvers of these warrants.

How secure do you consider that system within the framework of your knowledge of security functions throughout this country? Would you have a different system or an alternative system that you believe might be a more workable system or a more secure system or one that would be more beneficial to the legitimate security interest of this country?

Admiral TURNER. Without impugning the judges or anyone else in the system, it is axiomatic that the more people involved the more risk you take.

The bill does have provisions so that I, as the Director of Central Intelligence, would have a say in the procedures established for the communication and establishing a repository for the judges of this material.

One never likes to expand the quantity of people who have access to delicate information, but here again this is a delicate balance that we are talking about between finding a double check for the interests of our citizens and protecting the national interest.

Senator HATCH. Have you given any consideration to any alternative approach if that is even questionable in your mind?

Admiral TURNER. No; I have not been able to come up with any alternatives that would have any lesser risk. I think the risk here in this case could be minimized by procedures which we can establish.

Senator HATCH. So you consider this an acceptable risk and an acceptable approach. You expect that by the privileges granted you in helping to establish the procedures that we can have a basically risk-free security system; is that correct?

Admiral TURNER. I would never say risk-free, but we can have a satisfactory degree of risk or acceptable degree of risk.

Senator HATCH. Mr. Chairman, that is all I have.

Senator KENNEDY. I have one final point at this time.

Secretary Brown, in your testimony on the bottom of page 3 you talk about the question of a uniform system of accountability for all agencies and components of the intelligence community. You indicate the collection of foreign intelligence through electronic surveillance, like other aspects of our foreign intelligence activities, benefits from a diversity of approaches and the participation of different entities.

I am just wondering whether you feel, in the area of electronic surveillance, that such diversity is essential in terms of protecting the liberties of the American people as well as insuring our security.

Secretary BROWN. I believe that diversity of collection sources is important simply because different individuals or different agencies, although they need to be coordinated and supervised by a central

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

point, do have different needs and arrangements have to be made for them to make the collections that they need to make. I think that is very important.

That, however, makes it even more important that they all be required to abide by these procedures of the kinds set forth in this bill to give us assurance that those activities will be done under law and not used improperly.

I think that that diversity makes it even more important that a bill of this sort establish procedures the way things are done.

Senator KENNEDY. Admiral Turner, do you have anything to add?

Admiral TURNER. I agree completely with the Secretary.

Senator KENNEDY. Senator Abourezk?

Senator ABOUREZK. Thank you, Mr. Chairman.

I want to refer to what we have been calling the noncriminal standard section of the bill. Did I understand you to say that you do not favor the use of wiretap evidence under the noncriminal standard for prosecution?

Secretary BROWN. I do not think I said anything about that. I am not sure to whom you are addressing the question.

Senator ABOUREZK. Either one of you.

Admiral TURNER. I do not believe I said that, either.

Senator ABOUREZK. Let me then ask you this: The evidence gathered under the noncriminal standard of this proposed legislation can be used for prosecution in criminal cases. Do you have an opinion on whether or not such information ought to be allowed to be used in that way?

Secretary BROWN. The point that I would make about it, Senator Abourezk, is that before that is done the national security should be weighed in balance to make a determination whether the disclosure of the information would adversely affect national security to a degree that it outweighed the benefits to be gained by using the information in criminal prosecution.

Senator ABOUREZK. Do you have any doubt in your mind at all as to whether this kind of evidence might be unconstiutional, since it was obtained under a noncriminal warrant?

Secretary BROWN. I would want to leave that to the courts. I do not have a legal opinion on it.

Senator ABOUREZK. Are you concerned about it?

Secretary BROWN. I believe that the legal opinions from within the Department of Defense are that that is a constitutional use.

Senator ABOUREZK. Your view is that it is a constitutional use.

Secretary BROWN. Yes.

Senator ABOUREZK. Do you know, either Admiral Turner or Secretary Brown, if there have been cases where the Justice Department has decided to use national security wiretap information for criminal prosecution where you think they should not have used it?

Secretary BROWN. I am not aware of any during my term in office.

Senator ABOUREZK. Were there any prior to your term, to your knowledge?

Secretary BROWN. I do not know. I am not aware of any during my term, and I think I would be. I do not know of any earlier ones but there may have been. Perhaps the DCI has knowledge of that.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Admiral TURNER. I would answer in the same way, Senator. I do not know of any, but I would only feel confident of that in the last 4 months.

Senator ABOUREZK. Could we ask both of you to have somebody search and submit that for the record? Would that be agreeable?

Secretary BROWN. Yes.

Admiral TURNER. Yes.

Senator KENNEDY. Without objection, it will be made a part of the record.

[Material to be supplied follows:]

Searches of CIA records did not surface any instances in which the Department of Justice used national security wiretap information for criminal prosecution where CIA did not think the Department should have used it.

DEPARTMENT OF DEFENSE,
OFFICE OF GENERAL COUNSEL,
Washington, D.C., June 29, 1977.

Mr. KENNETH FEINBERG,
Staff Member, Office of Senator Edward M. Kennedy,
U.S. Senate,
Washington, D.C.

DEAR KEN: Subsequent to the Secretary of Defense's testimony on S. 1566 before the Subcommittee on Criminal Laws and Procedures of the Senate Committee on the Judiciary, you and I spoke on the telephone to clarify the Subcommittee's requests for additional submissions. The responses to these specific requests are set forth below:

Question 1. What example can be submitted by the Department of Defense to establish the need for the non-criminal standards of S. 1566?

Answer. The non-criminal standard is a very narrow exemption that would be applied in the limited circumstances such as the example on pages 22 and 23 of the Report of the Select Committee on Intelligence, 94th Congress, 2d Session. This provision is included in the Bill to compensate, in part, for the difficulties in securing warrants to conduct electronic surveillance to investigate violations of the espionage statutes. Generally, the non-criminal standard would be relied upon in the situation where a United States employee engaged in sensitive intelligence duties contacts a foreign agent, acts pursuant to the agent's direction, and is seen passing information to the foreign agent in a covert or clandestine manner. If the Government has no means of knowing whether the information passed is "national defense information," as required by the espionage statute (even though that is suspected to be the case), it could not make the requisite showing of probable cause that a crime has been committed, but the Government would be permitted to apply for a warrant under the non-criminal standard.

Question 2. Would the Department of Defense concur in a provision of S. 1566 to require Attorney General approval to allow continuance beyond a 90-day time limit for testing activities for counterintelligence purposes to uncover the electronic surveillance operations of foreign powers or their agents?

Answer. While the Department of Defense would have no objection to a 90-day time limit for testing the capability of electronic equipment, we would not concur in a time limit being placed on counterintelligence activities to uncover the electronic surveillance operations of foreign powers. 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.

Question 3. What explanation supports the Department of Defense position that all foreign intelligence surveillance operations conducted solely within the United States could not be conducted entirely by the FBI?

Answer. The foreign intelligence electronic surveillance activities conducted by NSA within the United States require a cryptologic capability that is closely

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

linked with such activities overseas and often require very time-sensitive information handling procedures. Involvement of the FBI in these activities would be a substantial departure from its law enforcement responsibilities.

Question 4. Can details be furnished in an unclassified written form regarding the six new electronic surveillance operations since Secretary Brown took office for which the Department of Defense requested Attorney General approval? If these details cannot be furnished in an unclassified written form, can Secretary Brown personally discuss these matters with Senator Kennedy?

Answer. It is not possible to provide an unclassified written explanation; however, Secretary Brown is prepared to brief Senator Kennedy personally.

Question 5. Would Secretary Brown submit his views generally in writing regarding the issue of centralization of the Intelligence Community? Would Secretary Brown be willing to personally discuss this issue with Senator Kennedy?

Answer. The Administration is actively engaged in a review of the organizational structure of the Intelligence Community. There are a number of different organizational options being discussed, but the written presentations about these options were prepared for the NSC and authorization for their release would most appropriately come from Mr. Brezezinski. Secretary Brown is willing to discuss these options with Senator Kennedy at the Senator's convenience. My office will set up an appointment next week if that is convenient.

Question 6. In how many instances has information acquired from electronic surveillance been used by the Department of Justice in court, over the objection of the Department of Defense, in a manner that created risks for national security?

Answer. The purpose of the national security clause in Section 2526(a) of S. 1566 is not to prevent the Justice Department from taking action to prosecute cases, but to recognize that a balancing process should take place within the Executive Branch. This legislation is a codification of processes previously carried on entirely within the Executive Branch and, as such, shall include express Congressional recognition of the balancing process as well.

Question 7. Why does the definition of electronic surveillance found in Section 2521(b)(6)(A) include the term "particular, known United States person" when other sections use only the term "United States person?"

Answer. It is our understanding that the Department of Justice has submitted extensive comments on this question in the form that is attached. The Department of Defense concurs in this position.

Sincerely,

GERARD V. D'ALESSIO, Jr.

Attachment.

DEPARTMENT OF JUSTICE RESPONSE TO QUESTION 7

The word "known" in Section 2521(b)(6)(A) refers to the intelligence agency's knowledge. It is necessary because radio communications are targeted which are known to orginate from or be received in the United States, but the identity of the person involved is totally unknown and largely undiscoverable. This activity is currently governed by the Attorney General procedures to assure that it is only done in proper cases and that there is minimization of the acquisition, retention, and dissemination of the information acquired to that which is necessary for foreign intelligence purposes. These procedures would continue to apply after the passage of S. 1566. As to possible deliberate evasion of the bill's requirements by avoiding discovery of who the person is, I can assure you that a high priority of this activity is in fact to discover the identity of the communicator. If, finding that the person was a United States person, the applicable agency failed to immediately obtain a warrant—if a warrant were required for law enforcement purposes—the agency would be as criminally liable as if they had otherwise engaged in electronic surveillance in violation of the chapter.

The situation may also arise where in good faith an intelligence agency is monitoring the international radio communications of a foreign government official who comes to the United States. Under the bill this would not require a warrant. It is possible, however, that such a foreign official could be a United States citizen. It is not unheard of for United States citizens to emigrate to a foreign country and then become an official of that country after several years. Although the law in this area is not entirely clear, generally, unless an American citizen expressly renounces his citizenship, he does not lose his citizenship by becoming a citizen of a foreign country. Where this situation is known to an

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

intelligence agency, the agency would be required to obtain a warrant under this bill if such a citizen came to the United States, but the situation has arisen where only substantially after the fact has the person's American citizenship became known. Therefore, the qualifier "known" is required to keep such a mistake from becoming a criminal offense.

Senator ABOUREZK. A new section has been added to the definition of electronic surveillance in the bill this year. I want to refer you to page 6 of the legislation, line 18, which says "intended to be received by particular, known U.S. person who is in the United States." It relates to NSA intelligence activities when directed against a particular known U.S. person.

There are several other places in the bill where "U.S. person" is distinguished from other persons, but nowhere else in the bill is that phrase modified by the qualifying word "known."

It contemplates that before surveillance activities are directed against any individual the investigating agency would have to already have determined that the target is a U.S. person since different standards and procedures apply.

Is there any reason why we should not strike the word "known" on page 6 as surplus language? Is there any reason to have that word in there?

Admiral TURNER. My view quickly is only that it tends to emphasize the fact that this must be a U.S. person here. I have not thought about whether there is some other implication for deleting it. I thought it was helpful for emphasis.

Senator ABOUREZK. Don't you think it would be confusing to a court trying to interpret this law?

Secretary BROWN. I think I can say a little more about that, Senator Abourezk.

In many of these cases it cannot be said in advance who the individuals are. It simply is not known because many of these channels of communication are used by a great many people.

Using the word "known" does allow a standard to be set. Without that I think the standard is much less clear.

Senator ABOUREZK. Then why do we not use the word "known" throughout the bill? Why is it just used in that section?

Miss SIEMER. Perhap I can comment on that, Senator. The definition of electronic surveillance, as you know, is keyed to what kind of disclosures have to be made with respect to what kinds of powers and what kinds of agents. The bill is drafted in other sections to accommodate our problem with associations of persons, substantial numbers of whom have U.S. connections, and U.S. corporations which are incorporated here which have substantial numbers of U.S. persons associated with them.

This is intended to get at a problem that we have with bulk communications.

Senator ABOUREZK. With what kind of communications?

Miss SIEMER. Bulk communications. Those are communications which are not simply from one person to another person or one entity to another entity, but they include large numbers of communications and large numbers of subjects.

The particular problem with that was addressed by the Attorney General.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

A more precise explanation as to why that is necessary, I think, would be appropriate for a closed session.

Senator ABOUREZK. Mr. Chairman, do you intend to have a closed session in order to obtain the answers to some of these other questions which you asked that were not able to be answered?

Senator KENNEDY. I think the Intelligence Committee is going to get into some of these aspects. I have no objection, but I think the Intelligence Committee would probably discuss these aspects. After the bill goes here, it goes over there. I think a closed session over there would probably be the best way unless the membership feels differently. I think we ought to get answers before we consider it on the floor. But are working closely with the other committtee.

Senator ABOUREZK. The answer to this question is that you have a reason for wanting that word in in that particular place but you cannot state it in open session; is that correct?

Miss SIEMER. I think the answer, Senator, is that it can be more completely explained with examples that would provide the basis for this language. This would be more appropriately done in a closed session.

Senator ABOUREZK. I think it is essential to explain it because it would be very confusing to any court trying to interpret this law at a later date if it were only in this one section and not in the other parts.

On page 27 of the bill, there are several provisions relating to the testing of electronic surveillance equipment. I want to ask you first if these particular provisions are of any interest to the Department of Defense or were they put into the bill at the request of some other agency or the CIA?

Secretary BROWN. They are of interest to the Department of Defense because we do carry out such tests, Senator Abourezk.

Senator ABOUREZK. Yesterday we discussed subsection (e)(1) on page 27, beginning at line 17, with the Attorney General. It was his testimony that this testing provision was not designed to cover the testing of so-called conventional electronic surveillance equipment, such as telephone wire taps or hidden microphones. Rather, he stated that this provision is intended to cover the design and development of highly sophisticated electronic equipment which can monitor communications from military aircraft and other essentially military sources.

After we discussed the fact that this provision is devoid of any limits on the nature of the test to be performed, the type of equipment to be tested, or the potential targets of the test, he agreed at the time we talked yesterday that that subsection is drafted too broadly and that certain restrictions probably ought to be written into it.

My question to you is this: Do you share the Attorney General's views as to the purpose of this section and the feasibility of limiting it to its intended purpose?

Secretary BROWN. I think the purpose can perhaps be defined more clearly, Senator Abourezk. The limitations on such tests, which as it says here include destroying the contents of the communications that is acquired are such a test, and limiting it to 90 days except with the prior approval of the Attorney General, take care of the problems of potential abuse.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

This section covers some advanced methods. Again, I would not want to go into detail here. Indeed, in some cases it is work on which research is just now being done.

I think it would be a mistake to write in limitations on the details that these provisions which call for the nonuse of the material and destruction of the material so collected should be able to take care of the abuse question.

In particular, I think it is important that we not limit this section because much of this work is aimed at protecting U.S. persons from foreign surveillance.

Senator ABOUREZK. Granted, that is your intention at this point but the language is pretty clear, to me at least, that it allows testing of any kind of electronic equipment which to me would include wire tapping and bugging, not only the sophisticated military things about which you are talking.

If it does that, what is to stop the Government, for example, from testing some new wiretap equipment on Mort Halperin. Granted again, they destroy the tapes right away but, based upon that tap, they go into court and say, "Well, we have heard something on that test tap that we have had so that we have probable cause now to go in for a warrant." That is what I am talking about by way of limitation.

Secretary BROWN. The Defense Department intelligence gathering activities that are under my cognizance do not include wiretapping or bugging. That kind of limitation, therefore, would not affect what we have in mind. I am not sure what trouble other agencies of government might have with that.

Senator ABOUREZK. Justice yesterday laid it all off on the military, or most of it. They said they did not mind narrowing down the provision.

Secretary BROWN. What I am saying is that exclusion of wiretapping and bugging was not our intention.

Senator ABOUREZK. Admiral Turner?

Admiral TURNER. The example given by Justice yesterday is not expansive enough for the test operations that are required by the intelligence community as a whole, Senator.

Wiretapping and bugging are not necessary for the intelligence community testing at this time because we can do that with a simulator. That is how we do it. We create an artificial transmission and do that testing.

I would have some reluctance, but I would not stand and bleed on having that eliminated from here, only because of future technical things that I cannot forecast or predict.

The principal provision not covered by the definition given by Justice yesterday, sir, concerns what we call signal processing. That is an ability to take a very busy, confused signals atmosphere, such as all of the signals that might be passing through this room right now—radios, televisions, radar, and so on—and being able to segregate out from that the signal, particularly a very weak signal, that you happen to want. You need an environment, an atmosphere, to do this much less restrictive than what was defined by the Justice people.

We could go overseas and do that testing. It is a matter of cost and convenience and establishing laboratories and getting permission from foreign powers, and so on.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

These techniques are something you just have to play with and work with. It is a major effort. It is one of the great accomplishments of our country in the technical field today.

Senator, if in this process we specifically picked Mort Halperin and said, "Let's test it on him," we are violating the law by so doing. We are violating this law.

Senator ABOUREZK. I do not read it that way, Admiral. Under this proposed law you are entitled to test on anybody without a warrant.

That is why I want a restriction in it. As I understand your testimony, you do not really have much of an objection to that particular kind of restriction, just so your airwave testing is permitted under the law.

Admiral TURNER. I would be reluctant on restrictions as to the type of testing we can do. I would have no reluctance to insure that testing is not targeted against a U.S. person.

It would be my interpretation, though, that if you set out with that particular objective in mind you would have to go through the warrant procedures that are provided for in the law. I am not a lawyer, so I leave that to you.

If there is tightening up in that regard, I have no objection.

Senator ABOUREZK. On page 28, I have one more question, beginning on line 3.

I wonder if either or both of you could explain to the subcommittee why section (e) (ii) is necessary and what it is designed to accomplish.

Admiral TURNER. This is to protect us against intrusion by audio techniques of other powers. Were this a classified hearing, Senator, we would have had someone come in here half an hour before the hearing or at some random time to check that nobody had planted a bug in here. We do this in many places where we have a defensive requirement against intrusion.

Senator KENNEDY. Did you do it here this morning?

Admiral TURNER. This is not a classified hearing, Senator. We would have done it otherwise; yes, sir.

Senator ABOUREZK. Thank you very much.

Senator KENNEDY. Secretary Brown, why should the NSA be doing any wiretapping whatsoever here? Why don't we just say that within the United States if we are trying to get control over this particular problem in ways that are going to secure our national security and also protect the civil liberties of the American people—why shouldn't that surveillance only be done by the Federal Bureau of Investigation?

Would you have any objection to an amendment that would insure that any electronic surveillance in the United States is going to be accomplished by the Federal Bureau of Investigation?

Secretary BROWN. Some of the kinds of activity about which you are talking, Mr. Chairman, are very highly technical and related to other activities and some of these technical developments are more advanced than some of the agencies are prepared for.

The operators in the military agencies not only are accustomed to using very complex equipment, but it is the same equipment that is used for military purposes. Therefore, I think there is a considerable increase in efficiency in having the same people do those operations.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Senator KENNEDY. We are really talking about six, are we not? Those are the six new requests? How many of these six are being done by the NSA in the United States?

Secretary BROWN. I think that should not be said in open session.

Senator KENNEDY. We heard from the FBI. They indicated there were 77 surveillances, all of foreign powers, none on American citizens. That is not going to have much relevancy if we are not able to get similar information from your office.

Secretary BROWN. The number for DOD activities of course is less than that. Ours are includde in that. They do not constitute the total number you were given.

Senator KENNEDY. Are you suggesting you have a greater technological capacity in the areas in which you are operating within those 77 than the Federal Bureau?

Secretary BROWN. In many of these cases, of course, we ask that the Federal Bureau of Investigation carry them out.

Senator KENNEDY. Why not in all of them?

Secretary BROWN. I think it is a matter of the nature of the technology.

Senator KENNEDY. But we are talking about legislation now for the future. Are we wise to have a duplication of effort within the Federal Bureau if we are looking now towards the future?

Secretary BROWN. It is not infeasible but I do think it would require duplication of training, duplication of people, duplication of facilities.

Senator HATCH. They would still have to have AG approval, though, of every one of these.

Senator KENNEDY. Can you describe the distinction in closed session?

Secretary BROWN. I can try to write it out maybe even in an unclassified way, but I think it would be a mistake for me to try to say it in an unclassified way.

Secretary BROWN. It is a matter not only of detecting emanations of information, Mr. Chairman, whether wire, wireless, or whatever, but of building into the activities the kind of crytological techniques, the detailed analysis techniques, which the FBI really does not have at all.

Admiral TURNER. Mr. Chairman, I would be very happy to offer you a paper on this indicating the thing in detail.

Senator KENNEDY. I think that is important because we are attempting to identify responsibilities in these areas.

Admiral Turner, let me ask you a similar question. The Congress established very clearly that the Central Intelligence Agency should not be involved in surveillance here in the United States. Yet, as you mentioned earlier, you have an elaborate procedure by which you can get the Federal Bureau to do this kind of electronic surveillance, evidently following your procedures and at your request.

Why doesn't the Federal Bureau on their own initiate these wiretaps? Why should these requests come from the Central Intelligence Agency?

Admiral TURNER. That is an understandable point, Mr. Chairman. We must recall, though, that we are talking about foreign intelligence here. That is our objective.

Senator KENNEDY. In the United States.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Admiral TURNER. Collecting foreign intelligence in the United States, intelligence about foreign powers.

The FBI is not possessed of the knowledge as to what is the important intelligence to collect. Do we need more intelligence on the economics of country "X" or country "Y"? Do we need more intelligence on the political positions, on the military positions, and so on?

I believe that the direction, the requests for this information, must come from the intelligence community—from the CIA, the DIA, the State Department, the Bureau of Intelligence and Research, which are the basic analytic organizations of the intelligence community who know what our national requirements are to obtain information.

Senator HATCH. Don't you have difficulty handing off the information? If you were to transfer it to the FBI once a foreign situation comes into the country, wouldn't you have handing off problems? Wouldn't that complicate the intelligence approach? That might be very important to the country at that time.

Admiral TURNER. Yes, that is true, I think, largely in the counterintelligence field, Senator Hatch. We do have a handoff problem there although we have worked that interface reasonably well.

In the basic foreign intelligence field, however, I think it has to come, the direction has to come——

SENATOR KENNEDY. I could see where you could bring it to the attention of the Director of the FBI saying, "These are the matters with which we are concerned. We believe these are matters which are important." Then you let them make the judgment.

Admiral TURNER. As I see the procedures, sir, it is the intelligence agencies who develop the requirements and then it is this process, which presently, as I mentioned, includes an interagency review panel, the National Security advisor to the President, and the Attorney General, that validates whether the risk in getting that is worth it; whether the importance of the information is worth it; whether there could be alternative ways of getting the information without having to go through this.

Those are the checks on whether what the intelligence agencies are asking for are valid requirements for the Nation, and then injecting the FBI as the executor of that is the protection to the people that the intelligence agencies are not involved in obtaining information in the United States that could be improperly used. It gives protection or control by taking it out of the intelligence field and into the Attorney General's department.

Senator KENNEDY. We will explore this with the Director of the FBI.

This has been very helpful. Again we want to thank you.

Senator BAYH is a member of the full committee and has worked very closely with us in examining this information as well.

This bill is going to be sent to the Intelligence Committee and we want to move it in a satisfactory way.

We want to thank you very much for your appearance here this morning. Thank you, Mr. Secretary and Admiral Turner. We appreciate it very much.

Secretary BROWN. Thank you.

Admiral TURNER. Thank you.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Senator KENNEDY. Our next witness is Mr. John Shattuck, American Civil Liberties Union.

Mort Halperin, do you want to join Mr. Shattuck at the witness stand? We want to try to move the hearings along.

We want to welcome both of you.

Mr. Shattuck has long been interested in this legislation. We value very highly his opinions and views.

We look forward to your testimony.

Mort Halperin is the expert in terms of abuse. We obviously welcome his comments on this, too.

Mr. Shattuck, you may proceed.

STATEMENT OF JOHN SHATTUCK, AMERICAN CIVIL LIBERTIES UNION

Mr. SHATTUCK. Thank you, Mr. Chairman.

I would like to observe for the record that this is the first time in these series of hearings that I have ever had the opportunity of appearing before my client, Mr. Halperin. I consider it to be a very extreme privilege. I do not know how he views it.

I have submitted a statement for the record, Mr. Chairman. I will cover as many of the points in it as possible orally but also be as brief as possible.

The American Civil Liberties Union regards the issue before this committee as extremely important and far reaching, particularly in the context of the larger effort to bring the intelligence agencies under the rule of law in which this Congress is currently engaged.

It is in this bill, I think, that the Congress will draw the first line in this effort, but it is our view that as drafted the bill will not prevent a continuation of many of the abuses, or at least some of the abuses, that have been documented in the past.

The principal reason for this, Mr. Chairman, is that the bill in our view authorizes surveillance in a wide variety of circumstances in which there is no suspicion that a crime has been committed.

We are pleased that you and Senator Bayh, Senator Abourezk, and others on the committee are equally concerned about this aspect of the legislation and that you have indicated a willingness and desire to amend and improve the bill.

I would like to spend the bulk of my oral presentation this morning discussing this noncriminal standard in the legislation and to explain why we regard it as so important both as a matter of practical concern and as a matter of principle.

I think the best way to start is to just briefly look at the nature of wiretapping itself. Wiretapping, as you know, is the most intrusive form of search that has ever been devised. It is impossible to limit it, inherently impossible to limit it, in the way that many other kinds of searches can be limited.

This is dramatically demonstrated by statistics that were released just last week by the Administrative Office of the U.S. Courts, which show that the average court-ordered Federal wiretap in criminal cases in 1976 involved the interception of 1,038 separate conversations between 58 persons over a period of an average of 3 weeks. That

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

is, of course, criminal cases, not open-ended intelligence investigations for 90 days or 1 year as would be authorized by this bill.

Since wiretapping is therefore essentially and inherently incompatible with the 4th amendment as we know it, it should at the very least not be used at all unless there is probable cause to believe that a crime has been committed by the person who is to be tapped.

In fact, the whole history of the 4th amendment, Mr. Chairman, shows that a departure from the crime standard for intrusive searches, such as a wiretap, would be unprecedented. It has never occurred before.

When the 4th amendment was first adopted and for a long time afterward, the only searches that could be conducted were for contraband or other forms of material that were illegal to possess. When the Supreme Court abandoned that standard in 1967, it reiterated and restated as clearly as it could that a criminal nexus was still essential with respect to intrusive searches—less intrusive, I might add, than a wiretap.

In his testimony yesterday the Attorney General sought valiently but ineffectively to justify this bill's departure from the criminal standard by citing the so-called administrative search cases.

I think there are at least three reasons which I will just very briefly touch upon why these cases, most of which involved housing code violations, are simply not relevant to the context of wiretaps in S. 1566.

First, none of these cases represents a deliberate search for information totally unrelated to illegal activity. Searches even in the housing context are to find violations of housing codes.

Second, none of these cases dealt with sensitive communications or speech. Of course, that is the very content of the information to be seized in a wiretap.

Third, these administrative search cases deal with a much less intrusive form of search than the wiretap.

That is the only area in which there has been a departure from the crminal standard. I do not believe that a review of the cases would show that they are applicable to the situation here.

That is the criminal standard. Now let me briefly touch on the question of its application to foreign nationals who are in this country lawfully.

The Attorney General has argued, and so has the Secretary of Defense and the CIA Director, Admiral Turner, that foreigners and other foreign visitors are not entitled to the full extent of protection of the fourth amendment in this country. I don't think that assertion is borne out by a review of either the specific language of the fourth amendment or the cases which construe it.

The amendment refers to the rights of the people, not to the rights of citizens. It has been construed again and again to apply to all persons within the territorial jurisdiction of the United States.

In the leading case of *Abel* v. *United States*, in which a Russian spy challenged the search of his apartment which led to his espionage conviction, in that leading Supreme Court case there was no question that the fourth amendment was considered to apply even to the case of a known and convicted Russian who was engaged in espionage.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

The Court affirmed that conviction by finding that the search was incidental to a valid deportation arrest. That is true.

The important point is that throughout the decision, both in the majority and the dissent, it was assumed that even those who engaged in espionage and who were illegally in this country were entitled to fourth amendment protection.

With respect to deportation arrests, the probable cause standard is, in fact, lower. That is only in the case of deportation arrests. If there is someone illegally in the country who is to be deported, there is less than probable cause that needs to be shown in order to arrest that person and deport him or her.

At the time that any other activity is engaged in by someone who is an alien, the full extent of fourth amendment protection goes.

With respect to foreign embassies and employees, which is another very troubling question in the long deliberations over this bill, the Federal courts have for a long time recognized the duty imposed by international law to protect the residence of an ambassador or minister against any invasions or any other kind of searches.

This has now been embodied in the Vienna Convention on Diplomatic Relations, which was ratified by the Senate in 1965.

It in no uncertain terms says:

> The premises of the mission, their furnishings, and other property thereon, and the means of transport of the mission shall be immune from search, requisition, attachment, or execution.

So, in order to establish a broad noncriminal standard to apply to a range of foreigners as well as American citizens it is necessary to go around not only the fourth amendment, but international law and specifically the Vienna Convention.

Mr. Chairman, I will not review the four separate classes of persons who are subject to surveillance on a noncriminal standard under this bill, because you are certainly familiar with that.

I would like to conclude my oral presentation by simply looking beyond the noncriminal standard and stressing, as I did at the outset, that we are really dealing with much more than the wiretap bill. We are dealing ultimately with the question of what standards are going to be set for the control of the intelligence agencies.

If in the case of a wiretap surveillance, the most intrusive kind of surveillance that is known, a broad noncriminal standard is to be authorized, I think the implications of this are obvious. If the FBI is give an express authority to wiretap Americans and foreigners who are not engaged in crime, it will certainly assert similar and undoubtedly broader authority to conduct other investigations without any evidence of crime.

It is for these reasons that we oppose the bill in its current form and urge that the committee adopt the amendments that we recommend at the back of my statement, some of which Mr. Halperin will be explaining in further detail in his testimony.

I will yield to him in the interest of time and hope that my full statement will be made a part of the record.

Senator KENNEDY. It will be made a part of the record.

Mr. SHATTUCK. Thank you.

[Material follows:]

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

STATEMENT OF JOHN H. F. SHATTUCK, DIRECTOR, WASHINGTON OFFICE, AMERICAN CIVIL LIBERTIES UNION

Mr. Chairman: I am pleased and honored to appear before this Subcommittee to testify on a subject of vital concern to the American Civil Liberties Union. I am an attorney and the Director, Washington Office of the ACLU, a nationwide, non-partisan organization of 275,000 members, devoted to protecting individual rights and liberties guaranteed by the Constitution.

As an ACLU attorney I have served as counsel in several lawsuits challenging federal wiretaps on American citizens undertaken in the name of national security. In two of these cases courts have recently held that the Fourth Amendment was violated by warrantless surveillance allegedly conducted to protect the foreign security of the United States. *Halperin* v. *Kissinger*, —— F.Supp. —— (D.D.C. 1976). In my view these cases demonstrate graphically the essentially uncontrollable nature of wiretapping under a vague foreign intelligence standard when there is no probable cause to believe that the target of the surveillance is engaged in crime.

S.1566, the bill under consideration in these hearings, fails to cure this essential defect. Unless the bill is amended to limit all wiretaps to a criminal standard, it will constitute a step backward in Congress effort to bring the intelligence agencies under the control of the Constitution. While the bill is an improvement over its predecessor, S. 3197, in that it implicitly rejects any assertion of an inherent presidential power to circumvent the law, it is still fundamentally flawed because it fails to satisfy basic requirements of the fourth amendment. Like its predecessor, S.1566 again poses the stark question: Will the Congress, in an illusory reform, participate in cutting back the Bill of Rights in the name of essentially undefined intelligence interests?

We are pleased that Senators Kennedy and Bayh, two of the principal sponsors of S.1566, have identified a variety of serious problems in the bill, including its departure from a criminal standard, and have expressed a desire to improve the legislation substantially. We urge the Committee to make these and other improvements which are set forth in the second part of my statement. First, however, I would like to explain in detail why the bill's failure to follow the criminal standard of the fourth amendment renders meaningless its claims of reform and makes it a potential legislative charter for intelligence abuses.

WIRETAPPING AND THE FOURTH AMENDMENT

A wiretap is probably the most intrusive and inherently unreasonable form of search and seizure. Even when a tap is placed on a person suspected of engaging in criminal activity, it offends the Fourth Amendment because it necessarily results in a "general search" of all private conversations, incriminating or not, which occur over the period of the surveillance. The surveillance technology itself severely impedes any kind of effective control, such as a conventional search warrant which (1) authorizes the seizure of tangible evidence, (2) "particularly describes" the things to be seized, and (3) gives notice to the subject of the search except under narrowly defined "exigent circumstances." Cf. *Osborn* v. *United States*, 385 U.S. 323, 329–30 (1966).

The technology of electronic surveillance makes the search and seizure of telephone conversations infinitely more intrusive than the physical search of a home or a person, even when a tap is conducted pursuant to a court order. Statistics released recently by the Administrative Office of the U.S. Courts, for example, show that the average court-ordered federal wiretap in 1976 involved the interception of 1,038 separate conversations between 58 persons over a period of three weeks. These statistics demonstrate dramatically that even in the case of a criminal investigation—far more limited than the open-ended 90 day or one year "intelligence" investigations authorized by S. 1566—a wiretap search inevitably has a dragnet effect which strains the Fourth Amendment to the breaking point. Electronic surveillance, therefore, is the prime example of Justice Brandeis' foreboding in *Olmstead* v. *United States*, 277 U.S. 438, 473 (1928) that "discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." Even where circumscribed within the confines of a criminal investigation, wiretapping represents an intensive and extensive invasion of private speech and through with almost no parallel. Wiretap devices intrude

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4
93-179 O - 77 - 6

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

so deeply and so grossly, they discourage people from speaking freely, and, as Justice Brennan has warned, if such devices proliferate widely. we may find ourselves in a society where the only sure way to guard one's privacy "is to keep one's mouth shut on all occasions." *Lopez* v. *United States*, 373 U.S. 427,. 450 (1963).

A CRIMINAL STANDARD: THE MINIMAL CONSTITUTIONAL REQUIREMENT FOR WIRETAPS

Since electronic surveillance is inherently so intrusive, the ACLU has long maintained that it cannot be conducted at all without violating the Fourth Amendment. If this violation is to be minimized, at the very least no surveillance should be authorized unless there is probable cause to believe that the person to be tapped is engaged in crime. The Fourth Amendment stands as the fundamental constitutional protection of the right of privacy—the right to be left alone in the absence of a compelling societal interest mandating the intrusion. *Katz* v. *United States*, 389 U.S. 347 (1967). It says, in effect, that the government is not authorized by the people to invade their privacy without a sound basis for believing that a crime has occurred and that evidence of this crime will be obtained in the search.

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause. . . ." In the debate over S. 3197 and S. 1566, the question is "probable cause" to believe what? That a crime has been committed? Or, can a search fulfill the probable cause requirement in the absence of a connection to criminal activity?

This is not a question which would have occurred to the Framers of the Fourth Amendment. In accord with English common law, *Entick* v. *Carrington*, 19 *How.St.Tr.* 1029 (1765), they believed that a warrant could issue only for contraband, or fruits or instrumentalities of a crime. "Mere evidence," such as private papers of an individual, could not be seized with a warrant under any circumstances. *Gouled* v. *United States*, 255 U.S. 298 (1920). Warrants were entangled with concepts from the law of property. The government could only seize those items that the possessor could not lawfully possess.

But those items subject to seizure—contraband, fruits and instrumentalities—all presuppose that a crime has been committed. It is criminal to possess items declared to be contraband, such as narcotics. Fruits of crime, such as stolen goods, also presume the existence of a crime. And it was, and is, a crime in itself to possess certain instrumentalities, such as burglar's tools. Thus, the Framers could not even have conceived of a search not related to criminal activity. Although they did not talk in terms of probable cause that a crime has been committed, a search was permissible only if there was probable cause to believe that certain items, intimately associated with crime, could be found at the place to be searched.

In 1967, the Supreme Court abandoned the prohibition against the search for and seizure of "mere evidence." *Warden* v. *Hayden*, 387 U.S. 294 (1967). The permissible objects of a search were no longer limited to contraband, fruits and instrumentalities. However, the Court did not intend—nor would the history of the Fourth Amendment support—abandonment of the criminal standard:

"There must of course be a nexus—automatically provided in the case of fruits. instrumentalities or contraband—between the item to be seized and criminal behavior. Thus, in the case of 'mere evidence,' probable cause must be examined in terms of cause to believe that the evidence sought will aid in a particular apprehension or conviction." *Id.* at 307.

Thus, even while abandoning the mere evidence rule, the Court explicitly retained the requirement that a relationship be demonstrated between the object to be seized and activity in violation of the criminal laws.

Those who would justify a departure from the criminal standard quote the following passage from Justice Powell's opinion in *United States* v. *United States District Court*, 407 U.S. 297, 322–323 (1972):

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

Justice Powell's dicta are based on the administrative search cases. In these cases, see e.g., *Camara* v. *Municipal Court*, 387 U.S. 523 (1967), *See* v. *Seattle*,

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

387 U.S. 541 (1967), the Court sanctioned the use of area warrants whereby municipal authorities might inspect a business or a dwelling for housing code violations, not upon probable cause that the dwelling was in violation of a particular housing code provision but upon general experience that dwellings in a particular area are likely to be in violation of the code.

The administrative search cases are a weak reed upon which to rest such a dangerous relaxation of Fourth Amendment standards. None of these cases in fact represents a deliberate search for information unrelated to criminal activity, as does S. 1566. The searches were to enforce and find criminal violations of the housing code. Second, none of these cases deal with potentially sensitive political activities. The Court has recognized the convergence of the Fourth and First Amendments: "Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power." *Marcuh* v. *Search Warrant*, 367 U.S. 717, 724 (1961). In *Keith* itself, the Court emphasized this relationship. *United States* v. *United States District Court*, *supra* at 313. Third, the administrative search cases deal with a much less intrusive invasion of privacy. A walk-through of a dwelling seeking compliance with a housing code is hardly comparable to 90 days of electronic surveillance gathering every communication—whether or not relevant—made from a partcilluar facility. The degree of instrusivenss is the decisive factor in determining the quality and degree of justification that must be provided for a search. A wiretap, of course, is the most intrusive of all searches and therefore requires strict adherence to the criminal standard.

FOREIGN NATIONALS AND THE FOURTH AMENDMENT

It is often argued that foreign visitors and employees of a foreign power in the United States are less protected by the Bill of Rights than American citizens and resident aliens. This is the premise of S. 1566. There is little basis for it in constitutional law.

The Fourth Amendment, of course, refers not to the rights of citizens or residents, but the "right of the people" to be free from unreasonable searches and seizures. Just as the term, "person," in the Fifth Amendment has long been held to be "broad enough to include any and every human being within the jurisdiction of the republic," *Wong* v. *United States*, 163 U. S. 228, 242 (1896) (Field, J., concurring), the "people" who are protected by the Fourth Amendmend have been held to include all persons within the territorial jurisdiction of the United States. More than fifty years ago, for example, the Supreme Court estabilshed that an alien could invoke the exclusionary rule in a deportation proceeding. *Uniced States ex rel. Bilokumsky* v. *Tod*, 263 U.S. 149 (1923). The extension of full Fourth Amendment protection to foreign nationals has been long and repeatedly recognized by lower courts, e.g. *In re Weinstein*, 271 F.5 S.D.N.Y. 1920), aff'd, 271 F.673 (2nd Cir. 1920) (Learned Hand, J.) and has most recently been noted by the Supreme Court in *Abel* v. *United States*, 362 U.S. 217 (1970). *Abel* involved a joint investigation by the FBI and Immigration officials of a suspected Russian spy. A search was made of the suspect's hotel room at the time of his administrative arrest preliminary to deportation with the FBI conducting a subsequent search on its own. These searches turned up not only proof of Abel's alienage and illegal entry into the United States, but of espionage (coded messages, microfilms), and the government brought an espionage prosecution and obtained a conviction. Abel appealed on the ground that the evidence on which he was convicted was the fruit of an illegal search, and therefore should have been excluded.

The Supreme Court affirmed the conviction by finding that the search had been made incidental to a valid deportation arrest and was therefore legal itself. But the important point is that it was assumed by the majority (and stressed by the dissenters) that aliens, even those who had entered this country illegally and who were engaged in espionage, were entitled to full Fourth Amendment protection.

Although a deportation arrest may be based on less than probable cause, an alien who is investigated for purposes other than deportation is fully protected by the Fourth Amendment. As the Seventh Circuit Court of Appeals recently stated, plenary Congressional powers to deport aliens "cannot be interpreted so broadly as to limit the Fourth Amendment rights of those present in

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

the United States," *Illinois Migrant Council* v. *Pilliod*, 540 F. 2d 1062 (7th Cir. 1976). By the same token, the border searches of automobiles for illegal aliens on less than probable cause, see, e.g. *United States* v. *Martinez-Fuerte*, 96 S. Ct. 3074 (1976), cannot be taken to permit sweeping and intrusive non-criminal surveillance of foreign visitors anywhere in the United States.

The argument that foreign embassies and employees are in a class by themselves and can be subjected to broad surveillance, even if foreign visitors are protected by the criminal standard, is lacking in constitutional support and contrary to international law. There is little basis in Supreme Court caselaw for a distinction between types of foreigners lawfully in the United States. On the other hand, the federal courts have long recognized the duty imposed by international law to "protect the residence of an ambassador or minister against invasion as well as any other act tending to disturb the peace or dignity of the mission or the member of the mission." *Frend* v. *United States*. 100 F. 2d 691 (D.C. Cir. 1938), cert. denied, 306 U.S. 640 (1939). This obligation is more than a general principle of international law. The Vienna Convention on Diplomatic Relations, signed by the President and ratified by the Senate in 1974 expressly provides in Article 22 that:

"1. The premises of the mission shall be inviolable. The agents of the receiving State may not enter them, except with the consent of the head of the mission.

* * * * * * *

"3. The premises of the mission, there furnishings and other property thereon and the means of transport of the mission shall be immune from search, requisition, attachment or execution."

The Constitution expressly directs the President to carry out the laws and treaty obligations of the United States. Neither the Constitution nor the Vienna Conference Treaty will support the broad surveillance of foreigners which S. 1566 would permit. In considering the distinctions which the bill attempts to make, it is worth bearing in mind the Supreme Court's words of caution more than a century ago.

"The Constitution of the United States is a Law for rulers and people, equally in war and peace, and covers with the shield of its protection all classes of men, at all times and under all circumstances." *Ex Parte Milligan*, 4 Wall. 120, 121 (1866).

THE NONCRIMINAL STANDARD IN S. 1566

The absence of a crime standard was one of the principal issues on which S. 3197 foundered, and it is again the principal issue with respect to S. 1566. This bill authorizes wiretapping for three months or more of at least four classes of people who are *not* engaged in any criminal activity. First, the bill permits surveillance of officers or employees of a foreign power without any showing whatsoever that they are engaged in either criminal *or* intelligence activities. In effect, the bill declares open season on foreign employees of government corporations like Air France, who are subject to wiretap at any time simply because of their status. The second category of persons who can be tapped without any suspicion that they are committing crimes is foreigners engaged in undefined "clandestine intelligence activities" which might be harmful to the security of the United States. Apart from the bill's lack of definition of "clandestine intelligence activities," there is no evidence on the legislative record to indicate why the criminal standard of the espionage laws would not be sufficient to cover such persons. Under these circumstances it is difficult to see any objective limitation in the bill on the authority to tap foreign visitors.

The third category of persons covered by the non-criminal stnadard is Americans who secretly collect or transmit information pursuant to the direction of a foreign intelligence service "under circumstances which indicate the transmission or collection 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 complicated formula amounts to a new, all-inclusive and overbroad definition of espionage, with the result that the President is given the authority to wiretap Americans whose conduct has not been made criminal by Congress.

Finally, the most disturbing category of persons whose lawful conduct can trigger surveillance is Americans or foreigners who knowingly aid or abet persons

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

engaged in undefined clandestine intelligence activities or the secret transmission or collection of harmful information. These people are twice removed from the criminal standard: they can be tapped for aiding or abetting others whose conduct is lawful, and they need not even know the nature of that conduct so long as they are "knowingly" aiding the persons engaged in it. Under this standard Martin Luther King could arguably have been tapped, as he was, for "knowingly" associating with a person suspected of secret Communist activities, even though King knew nothing of those activities.

The inclusion of these four broad and vague categories of persons who can be wiretapped even though engaged in lawful conduct files in the face not only of the Fourth Amendment but also of the Church Committee recommendations and the criticisms levelled at S. 3197. It should be unnecessary to point out at this late date the extraordinary degree to which national security wiretaps have been repeatedly misused for political surveillance. The record of the Halperin litigation, *Halperin* v. *Kissinger*, *supra*, is but one example of the countless instances of illegal surveillance based on a non-criminal standard which have been exhaustively documented by this Committee and others. The Church Committee reviewed the problem carefully and concluded that the only protection against abuses was that "no American be targetted for electronic surveillance except upon a judicial finding of probable criminal activity." "Intelligence Activities and the Right of Americans, Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Book II, U.S. Senate, 94th Cong., 2d Sess., at 325 (1976). The Committee concluded that if the laws were insufficient "to cover modern forms of industrial, technological or economic espionage not now prohibited," then the laws should be amended, rather than create a new "dangerous basis for intrusive surveillance." Id. S. 1566, like S. 3197 before it, flatly ignores this recommendation.

The non-criminal standard in this bill would arguably permit an Attorney General insensitive to civil liberties to define "clandestine intelligence activities," or the secret collection or transmittal of national security information, to warrant electronic surveillance similar to the so-called "Kissinger seventeen taps" on journalists and government employees. Surveillance similar to the "sugar lobby" taps of a Congressman and his aides in the early 1960's (based upon an allegation that a foreign country was attempting to influence congressional deliberations about sugar quota legislation) would arguably be permissible. Political activity protected by the First Amendment could be reached in a variety of circumstances, such as the fund-raising activities of American religious and civic groups on behalf of Israel, or the receipt of an honorarium to speak to a foreign lobbying group. In short, the wiretap net could be cast very widely over non-criminal conduct under S.1566.

BEYOND THE CRIMINAL STANDARD: AUTHORIZING POLITICAL SURVEILLANCE

The importance of the criminal standard as a minimal constitutional requirement is based on considerations which go far beyond this bill. S. 1566 is the opening chapter in what should be a broad legislative effort to control the intelligence activities uncovered in recent years—such as the CIA's mailopenings, the FBI's cointelpro operations and "black bag" jobs, the IRS selective auditiing of "political dissidents," and other wholesale violations of constitutional rights—were justified on non-criminal national security grounds. Instead of rejecting this basis for surveillance. S. 1566 more firmly establishes it.

If the FBI is given an express authority to wiretap Americans not engaged in crime, it will most certainly assert a similar authority to conduct other investigations without evidence of crime. Under this approach the door to political surveillance is wide open. This was the principal concern expressed by Senator Walter Mondale when he testified last year in opposition to S. 3197:

"[T]he fact is that if you get the right of Government to investigate Americans for things that are not crimes, there are ways of destroying persons without ever appearing in a courtroom . . . [I]f you cloak an administration with an ill-defined power to investigate Americans outside the law, and in total disregard of their constitutional rights, it is inevitable that the police will be used to achieve political purposes, which is the most abhorrent objective and feat that we sought to avoid in the creation of the Constitution and the adoption of the Bill of Rights. So I think the enormity of the dangers here, particularly where we pass legislation to permit it—up until now it has been their fault, but now we

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

know, and if we authorize it from here on out, it is our fault." "Electronic Surveillance Within the United States for Foreign Intelligence Purposes," Hearings before the Subcommittee on Intelligence and the Rights of Americans, Select Committee on Intelligence U.S. Senate, 94th Congress, 2d Sess. on S. 3197 (June 29, 1976), at 56–57.

Senator Mondale as Vice President has been more willing to accommodate intelligence interests by abandoning his defense of the criminal standard at the risk of permitting the abuses he predicted. He and others who believe that such an accommodation is desirable should pause to review the history of similar compromises in the United States.

In May of 1798, less than a decade after the adoption of the Constitution, two of the Founding Fathers exchanged views on the problem of protecting both liberty and national security that would challenge the government they had created for the next two centuries. James Madison wrote to Thomas Jefferson:

"Perhaps it is a universal truth that the loss of liberty at home is to be charged to provisions against danger real or pretended from abroad."

One month after that letter was written, Congress enacted the infamous Alien and Sedition Acts, to protect American from European subversion.

The Alien and Sedition Acts were not reenacted and went into history within a short time after their passage, but they set a dangerous precedent for political repression in the name of national security. That precedent was repeated during the Civil War when Lincoln suspended the Writ of Habeas Corpus; during World War I and later in the Red Scare of the 1920's when "radicals" were persecuted by the federal government; and during World War II when the federal government incarcerated 120,000 Japanese-Americans in detention camps. Perhaps the most dangerous and threatening descendant of the Alien and Sedition Acts is the 40 year domestic intelligence program of the FBI that was so carefully documented by the Church Committee in their final report.

In every one of these cases, Congresses, Presidents and the American People were seduced by the argument that circumvention of the Bill of Rights was essential to protect the government from foreign subversion. S. 1566 perpetuates a basic element of that claim by relying on the assumption that limiting intrusive surveillance to criminal conduct is unworkable.

The Founding Fathers knew the answer to these arguments of necessity. The answer was provided by William Pitt, the famous English statesman of their age, who resisted similar arguments by the Crown on the floor of Parliament:

"Necessity is the plea for every infringement of human liberty. It is the argument of tyrants; it is the creed of slaves."

ACLU RECOMMENDATIONS

1. *§ 2521(b)(2)(A) (ii) and (iii) should be deleted*

Comment.—This provision is a wholly unacceptable effort to place foreign visitiors in a separate class. Such perons would include visiting relatives, students, businessmen, tourists and a limitless range of other lawful non-resident aliens. Since "clandestine intelligence activities" remains wholly undefined, the provision would subject foreign visitors to the possibility of wiretapping in a wide range of circumstances. Such individuals are not properly defined as agents of a foreign power and are entitled to the full protection of the Constitution and should be subjected to surveillance only under the same circumstances as apply to citizens and resident aliens.

2. *§ 2521(b)(2)(A)(i) should be amended as follows*

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

Comment.—As drafted the provision is vague and overbroad. The qualification "soon" is minimally essentially to prevent limitless surveillance of activities which are not in violation of the criminal statutes of the United States.

3. *§ 2521(b)(2)(B) (iii) and (iv) should be deleted*

Comment.—No person should be targetted for electronic surveillance unless there is probable cause to believe that the person is engaged in criminal activity. The Fourth Amendment requires no less in the case of a search as intrusive as a wiretap. Moreover, it is entirely possible to serve the purposes of a foreign

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

intelligence wiretap by applying the standard of 18 U.S.C. § 794, which makes it a crime to "communicate, deliver or transmit . . . to any foreign government, or to any faction or party . . . within a foreign country . . . or to any representative, officer, agent, employee, any . . . information relating to the national defense," if such action is taken "with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation . . ." A person or organization suspected of engaging in the crime proscribed by § 794 and could be wiretapped for foreign intelligence purposes.

4. *§ 2521(b)(6)(C) should be amended to delete the word "intentional"*

Comment.—The word "intentional" is an unnecessary qualification of "acquisition." It is not contained in subsections (A), (B) or (D) and should be deleted here.

5. *§ 2521(b)(8) should be amended to add the following provision at the end of the section*

"Information obtained under the procedures of this chapter from a United States person who is not the target of surveillance shall not be maintained in such a manner as to permit its retrieval by the name of that person unless it is: (*a*) evidence of a crime; (*b*) evidence that the person is a foreign agent eligible for surveillance; or (*c*) in a file maintained solely to respond to court orders related to electronic surveillance."

Comment.—One way in which national security wiretaps have been abused is by the storing of information in the files of Americans who are overheard on the surveillances of foreign powers. The minimization procedures in § 2521(b)(8) do not require minimization of surveillance of non-U.S. persons or of information related to the purposes of the surveillance. Information acquired from U.S. persons can be stored so that it is retrievable under the person's name unless it relates "only to the conduct of foreign affairs." The amendment is intended to protect U.S. persons against such storage and retrieval practices.

6. *§ 2521(b)(2) should be amended to provide as follows*

"United States person" means any person who is not an officer or employee of a 'foreign power' as defined by Section 2521(b)(1)."

Comment. See comment for amendment to § 2521(b)(2)(B).

7. *§ 2524(a) should be amended to provide as follows*

"Each application for an order approving electronic surveillance under this chapter shall be made by the Attorney General in writing upon oath or affirmation to a judge having jurisdiction under section 2523 of this chapter. It shall include the following information—"

Comment.—The requirement that all applications be made by the Attorney General was an essential element of the legislative scheme of S. 3197, and must be restored to S. 1566. Since the bill is a radical departure from the Fourth Amendment, no further erosion of constitutional safeguards should be permitted by allowing wiretap applications to be made by any "federal officer."

8. *§ 2524(A)(6)(7)(D), (7)(F), (8) and (10) should be amended to delete the clause, "When the target of the surveillance is not a foreign power as defined in section 2521(b)(1)(A), (B) or (C) . . ."*

Comment.—S. 3197 required a factual description of the nature of the information sought and the method of surveillance to be provided to the judge with respect to all wiretap warrant applications. If the warrant procedure is to have meaning at all, the judge should be told what information is sought in all circumstances.

9. *§ 2525(a)(5) should be amended as follows*

"(5) The application which has been filed contains the description and certification or certifications, specified in section 2524(a)(7) and [the certification or certifications are not arbitrary or capricious] *there is probable cause to believe that the certification or certifications are correct* on the basis of the statement made under section 2524(a)(7)(E)."

Comment.—One of the principal new features of S. 1566 is supposed to be that it "provides for judicial review of the certification by Executive Branch officials that foreign intelligence information is sought" [Justice Department Memorandum accompanying 4/27/77 Draft, p. 1]. This claim is inflated. The "arbitrary and capricious" standard of review is an inadequate standard for

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Fourth Amendment purposes. Unlike an administrative proceeding in which such a standard is applied, the warrant application is made in an *ex parte*, non-adversarial setting. If the warrant procedure is to have any meaning at all, the judge must be permitted to probe the certification to determine whether there is probable cause to believe that it is accurate.

10. § 2525(b)(1)(D) should be amended to delete the clause, "when the target of the surveillance is not a foreign power, as defined in section 2521(b)(1)(A), (B), or (C) . . ."

Comment.—The court should be required in all cases to specify in the order the means by which the electronic surveillance will be effected.

11. § 2525(b)(2)(B) should be amended to insert the word "may" between "person" and "furnish"

Comment.—Private persons should not be required to cooperate in placing surveillances. This provision should *permit* them to cooperate, thereby protecting them against liability. No penalty should attach to private persons who decline to assist in placing surveillances.

12. § 2525(c) should be amended to eliminate the one year authorization period for foreign power surveillance and limit all authorizations to ninety days

Comment.—The extraordinary intrusions permitted by this bill are dramatically demonstrated in the provision authorizing surveillance of foreign powers without review for one year periods. The ninety day periods permitted for United States persons are already far beyond the limits of any conceivable Fourth Amendment reasonableness.

13. § 2526(c) should be amended by deleting the last nine lines of the section, beginning with, "provided that, in making this determination . . ." and substituting in its place the following

"In making such a determination, the court, after reviewing a copy of the court order and accompanying application *in camera*, shall order disclosed to the person against whom the evidence is to be introduced the order and application, or portions thereof, if it finds that there is a reasonable question as to the legality of the surveillance and that such disclosure would promote a more accurate determination of such legality, or that such disclosure would not harm the national security. If the court determines that the electronic surveillance of the person aggrieved was conducted unlawfully, it shall turn over the information obtained or derived from the surveillance to such person. If the court determines that the electronic surveillance of the person aggrieved was conducted lawfully, it shall turn over a copy of the court order and accompanying application to such person only if the Government enters into evidence information obtained or derived from the surveillance."

Comment.—The procedure in the bill as it relates to the government using the fruits of an electronic surveillance in a trial raises serious *Alderman* and constitutional issues. Where the government seeks to use such evidence it should be required to disclose the warrant. Moreover, it is not sufficient for the court to suppress the evidence if illegally obtained; it must turn the evidence over to the defendant for a taint hearing.

14. § 2527 should be amended to add the following at the end

"(3) the periods of time for which applications granted authorized electronic surveillances and the actual duration of such electronic surveillances; and (4) the number of such surveillance terminated during the preceeding year."

Comment.—These important reporting provisions were contained in S. 3197 and should be reinstated.

15. Section 4(a)(1) of the conforming amendments should be amended to delete the clause, "as otherwise authorized by a search warrant or order of a court of competent jurisdiction"

Comment.—This clause would render meaningless the requirement that the procedures of this bill or Title III be followed for all electronic surveillances. Common law warrants which do not follow the procedures of this legislation should not be permitted to authorize any surveillance.

16. S. 1566 should be amended to prohibit surveillance of U.S. persons overseas except pursuant to the procedures of the bill

Comment.—The record of the Church Committee and the Senate Intelligence Committee indicates that there is a substantial amount of warrantless wire-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

tapping of U.S. persons overseas by federal intelligence agencies. The Constitution protects the rights of Americans overseas against actions by the U.S. Government, *Reid* v. *Covert*, 354 U.S. 1 (1957), and at least one court has held that warrantless wiretapping of Americans overseas is illegal under the Fourth Amendment. *Berlin Democratic Club* v. *Rumsfeld*, 410 F.Supp 144 (D.D.C. 1976).

Senator KENNEDY. Mr. Halperin, you may proceed.

STATEMENT OF MORTON HALPERIN, WASHINGTON, D.C.

Mr. HALPERIN. Thank you, Mr. Chairman.

I would like to focus on three issues. First, I would urge you to return at least to the language of S. 3197 as it relates to both the criminal standard and the non-criminal standard.

The testimony yesterday did not seem to me to make a case for these deviations other than to say that the Attorney General had looked at it again and wanted more authority. It seems to me you ought to have much more precise explanations for that.

In particular, I would call your attention to the conspiracy provision, which has not yet really been discussed, which simply says "conspires with or knowingly aids or abets any person engaged in the activities descibed above."

There is no conspiracy provision at all in the noncriminal standard in S. 3197.

Senator KENNEDY. Thay have agreed to change the language of the conspiracy provisions to return to last year.

Mr. HALPERIN. That is one. Let me go on to the others.

The noncriminal standard, it seems to me at a minimum——

Senator KENNEDY. We will have to interrupt. There is a quorum call in the full committee. We will recess briefly and then we will continue. I apologize, but we will come back.

[Recess taken.]

Senator KENNEDY. Mr. Halperin, you were testifying when we had to recess.

Mr. HALPERIN. Thank you, Mr. Chairman.

On the noncriminal standard, it seems to me we ought to all be able to agree that the Justice Department bears a very heavy burden if there is going to be a noncriminal standard. It is not enough to say that they will come out and think of a scenario of something that might happen that might be relevant. They really have an obligation to show that there is a very significant problem which may arise on a number of important occasions before we should depart from the criminal standard.

Senator KENNEDY. Wouldn't you agree with me that they did not meet it yesterday?

Mr. HALPERIN. I do not think they are anywhere near it. I think, in fact, all of the examples that they have given us so far over these five rounds now that they have been in things which are either trivial or covered by the criminal standard.

Senator KENNEDY. The espionage statute?

Mr. HALPERIN. Or the espionage, yes.

Given what the Supreme Court said in the *Gorin* case about the meaning of the phrase "national defense," a broad generic term of very broad connotation—the notion that you fit the other criteria of

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

the provision, that is, that you are a known espionage agent working for a hostile power secretly gathering information—then the question only is what is the information that you are secretly gathering. Given what the Supreme Court said about the pharse "national defense," if the judges would say that may be some information which is important but does not relate to national defense, it seems to me enormously remote—in fact, I think it is impossible to believe—that a judge would ever say, "You know he is a KGB agent, you know he is secretly gathering information; you know that the information's transfer to a foreign power would injure the United States, but you do not know that it is national defense within the meaning of the Gorin."

He does not have to have absolute certainty. He simply has to have probable cause to believe that the information relates to the national defense as it is very broadly defined.

If you look at the history of this, I think it suggests there is something wrong. Each time they have been before a committee they have had a different reason for wanting the noncriminal standard.

The first time they were here it was industrial espionage. Then when we showed that under *Gorin* industrial espionage was specifically included, they went on before the Senate Intelligence Committee to suggest that the real problem was that they did not know the content of the information. You do not have to know under 794 the content. You just have to know that it is related to national defense.

Then the first draft we got from the Justice Department this year had the foreign relations phrase in it, suggesting that they were trying to broaden it to foreign relations. They have now abandoned that. It is not in the text that was introduced.

They have introduced for the first time collection as well as transfer of information. At some point they seem to be suggesting that that was the reason they needed a noncriminal standard.

However, 794 has a conspiracy clause in it which says that if you are engaged in a conspiracy to transfer and you conduct any overt act looking toward the conspiracy to tranfer, then you have violated the law.

Again, we have a situation of members of a foreign intelligence service covertly collecting information pursuant to the direction of that service. Again it seems to me clearly there is probable cause to believe that the purpose of the collection is to ultimately transfer it to a foreign power. The foreign agent is not simply planning to keep the information for his own interests.

Therefore, you have a violation of 794(c), the conspiracy clause of 794.

I think that each time you look you find that the scenario they give would in almost every conceivable circumstance enable them to get a warrant.

The Attorney General, it seems to me, at the end was suggesting something quite different and quite disturbing. He thought a noncriminal standard meant lower standards of proof of the criteria that they had to meet.

As I read the bill, that is clearly not intended at all. The judge would have to find probable cause.

Senator KENNEDY. You read it correctly.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Mr. HALPERIN. Therefore, that distinction, which is what he seems to be suggesting was the reason for the noncriminal standard, again does not make any sense.

I am back to the issue that it is clear if you authorize any noncriminal standard you will be breaking the line against the effort to bring all the surveillance activities of the Federal Government under control by limiting it to a criminal standard. We may have to do that in certain circumstances for certain techniques dealing with Russian agents.

To do it for wiretapping, the most intrusive kind of surveillance, without a record which establishes the overwhelming importance of this, I think would be an enormous mistake. I think they are nowhere near meeting their burden.

I would like, if I may, to address one other issue. That is the question of minimization. I think the bill does not require any minimization. Indeed, I think the bill authorizes the worst abuse that occurred n the past, apart from targeting the wrong people.

I want to say, Mr. Chairman, I have appreciated the great concern about my telephone that has been expressed in the last few days.

The bill requires little minimization. Look at page 8, beginning on line 6. This affects only information which does not relate to the ability of the Unted States to do seven things. One of these is provide for the national defense or the security of the Nation.

Under this bill as written, if a U.S. Senator calls up a foreign embassy and discusses something that relates to the national defense or the security of the United States, there is no requirement at all for minimization. That information can not only be retained, but it can be put in the file of the U.S. Senator. When the White House asks for information about that U.S. Senator, that information can be transferred to the White House.

We know that that was done. Lyndon Johnson asked the FBI and later Richard Nixon asked the FBI what it knew about the views on Vietnam of U.S. Senators. That information was regularly provided to the White House.

I submit that this bill authorizes that kind of transfer of information.

Similarly, we know from the file of Richard Dudman, a Washington reporter, that the Government regularly picks up information about the phone conversations of reporters and it indexes it under the name of the reporter. Richard Dudman's file in the FBI had the text of many of his phone conversations with embassy officials of foreign governments.

Under this bill as it is now written, if that conversation relates to the national defense or the national security of the United States, the Government is authorized to file that information under Dudman's name and to use it for any purpose at all.

I think that the issue of minimization is not the minimization procedures, which are fine, but the fact that by the definition of minimization it excludes almost all the information which they pick up on these embassy wires.

I think it is very simple to prohibit that. I think that that is a change that should, in fact, be done.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

I have never heard an explanation from the Justice Department as to why they cannot file the information so that it is not retrievable under the name of the Senator. I am not proposing that they not be able to record the information in the file of the Soviet Embassy, or whatever it is that they are wire tapping so that they get a sense of what the Russians are doing, but I think they should be prohibited from filing that information so that it is retrievable under the name of a U.S. person.

Senator KENNEDY. The question here I suppose, is whether there is greater protection for the individual if it is retained to be used in a future lawsuit to show the abuses. How do you evaluate that—the dangers of destruction in terms of the Freedom of Information Act, for example, in terms of protecting an individual who may subsequently be involved in a lawsuit?

There is a question of whether it should be destroyed or retained. I am interested in your views and Mr. Shattuck's views in terms of the civil liberties question.

There have been those who feel that retaining it with the idea that it can be utilized in a future case provides additional protection. Others think it ought to be destroyed.

From a civil liberties point of view, I would be interested in your comments.

Mr. HALPERIN. My own view is that it should be retained because they may have, in fact, used it as a lead in a criminal case and then, if they destroy it, you have no way of going back and proving it.

We have a draft amendment attached to Mr. Shattuck's statement on the minimization provision. It provides three exceptions to the rule that you cannot index it so that you can retrieve it under the name of a U.S. person.

One is that it is evidence of a crime. One is that it is evidence that a person is a foreign agent eligible for surveillance under the terms of the bill, assuming that that was a noncriminal standard. The third is in a file maintained solely to respond to court orders relating to electronic surveillance.

In other words, if Dick Dudman is indicted, he has a right to know whether he was ever overheard and that information was used.

However, that index should be kept under secure conditions so that it only can be looked at for that purpose.

Senator KENNEDY. I think that is helpful. We will be glad to examine your suggestion.

Mr. SHATTUCK. I think our main concern, Senator, as you suggested is the dissemination and use of the material for purposes other than response to the Freedom of Information Act. To the extent that safeguards can be built in, then I think we certainly ought to go the route the amendment suggests.

Mr. HALPERIN. That completes my statement.

Senator KENNEDY. Fine. Your prepared statement in its entirety will be made a part of the record.

[Material follows:]

PREPARED STATEMENT OF MORTON H. HALPERIN

Mr. Chairman, I appreciate the opportunity to appear before this committee to testify on S. 1566.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

My remarks will be focused on two issues: the noncriminal standard and the indexing of information under the names of American citizens. First, I would like to make some brief comments on some other issues. I have a longer comment on S. 1566 which is to appear in the June issue of First Principles, the monthly newsletter of the Project on National Security and Civil Liberties. It is attached to my statement and I request that it be included in the record along with the written version of my statement.

John Shattuck is submitting to you a list of amendments with which I wish to associate myself. In particular, I urge this committee as a minimum to restore the provisions of S. 3197 as they relate to the criteria and categories for determining who may be surveilled. This means: (1) eliminating the special provisions for embassy and embassy-related surveillances, (2) eliminating the special new category of non-U.S. persons, (3) restoring the tight conspiracy clause in the criminal standard paragraph, and (4) restoring the previous language of the noncriminal standard paragraph and eliminating any conspiracy provision.

I would also urge you to look hard at the criminal standard paragraph and to tighten it up by defining clandestine intelligence, and specifying a list of crimes which would trigger this provision.

Noncriminal Standard

Mr. Chairman, for many months now I have sought to understand why the FBI and the Justice Department insist that there can be no bill unless they are authorized to conduct some surveillance of American citizens who are not suspected of criminal activity. I remain as perplexed as I was at the beginning. None of the reasons advanced for this proposition appear to me to be serious, and I have been forced to the conclusion that the purpose remains unstated.

When the legislation was first introduced, it was said that the need for the noncriminal standard related to industrial espionage. The report of this committee put the matter as follows:

> On the basis of testimony of, and discussions with, the Department of Justice, the committee agreed to include within the intended meaning of "clandestine intelligence activities" certain narrowly circumscribed intelligence activities closely related to criminal espionage but not presently constituting an offense under Federal law.
>
> The main category included within the scope of this phrase would be the hostile clandestine collection of industrial or technological information by a member of a foreign power's intelligence network which presents a significant threat to the national security of the United States. The Attorney General testified that current Federal espionage laws do not adequately cover situations in which the national security interests of the United States are impaired by the hostile clandestine collection of such information.
>
> * * * * *
>
> "The other category of noncriminal activity included within the intended definition of "clandestine intelligence activity" is so-called "third country" spying. If an American in this country joins the intelligence agency of a foreign power and proceeds to gather intelligence about one foreign government on behalf of another, this might constitute "clandestine intelligence activity," even though the espionage is not directed against the United States Government and does not, therefore, violate the espionage laws. Once again, however, this activity constitutes clandestine intelligence activity only if such third country espionage activity thereby endangers the national security or foreign relations of the United States. It does not include protests, demonstrations, or other such lawful political activity directed against a third country, even if carried out at the direction of a foreign power.

The first of these categories relating to industrial espionage, which received the most attention, simply cannot stand up under scrutiny. The espionage law as interpreted by the Supreme Court clearly covers the gathering of such information. 18 U.S.C. 794 reads as follows:

> § 794 *Gatherin or delivery defense information to aid foreign government*
>
> (a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, com-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

municates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or imprisonment for any term of years or for life.

(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

The Supreme Court, in *Gorin* v. *U.S.*, 312 U.S. 19 (1941), stated: "National defense, the Government maintains, 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.

If a court found that a person fit all of the other requirements of 2521(b)(2)(B)(iii) 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.

By the time that the Senate Intelligence Committee considered the matter, the rationale for the noncriminal standard had changed. That report described the situation as follows:

Subparagraph (E) encompasses the third class of "targetable" persons who are involved in clandestine intelligence activities. This subparagraph reflects the only situation in which a permanent resident alien or citizen of the United States may be surveilled even though the Government cannot establish that he is involved in specific criminal activity. It is the committee's judgment, however, that this subparagraph contains standards sufficiently stringent so as to afford an extremely high standard of protection consistent with 4th amendment requirements. The committee has also concluded that this restrictive class of "targetable" persons is essential to Government's ability to protect itself against the clandestine intelligence activities of a hostile foreign intelligence service.

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

That explanation assumes that it is necessary to know precisely or even generally what the content of the information is to establishing what law is being violated, if any, in order to secure a warrant. However, 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." Moreover, the conduct described in the Senate Intelligence Committee would involve a violation of 18 U.S.C. § 794. Given the very broad interpretation given to 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.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

When the Carter administration came into office there was, we are told, a careful reevaluation of this entire question. Unfortunately, neither a decision to abandon the noncriminal standard nor a clear statement of why it is needed has emerged.

The first draft circulated by the new administration made two significant changes in the language of the noncriminal standard. It added collection to transmission and injury to the foreign policy to injury to national security. The latter did move significantly beyond current law since it is not now a crime to traffic in information that affects "foreign policy" unless it also affects "national defense." However, this change was abandoned in S. 1566.

The "collection" provision remains in and the suggestion now appears to be that this is the essential deviation from the criminal standard. However, this argument ignores 18 U.S.C. § 794(c) which reads as follows:

> (c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy. As amended Sept. 3, 1954, c.1261, Title II, § 201, 68 Stat. 1219.

If a person were surreptitiously collecting information pursuant to the direction of an intelligence service or network, there would be probable cause to believe that he or she were conspiring to transfer information and that the collection was an act to effect the object of the conspiracy. (If there were any doubt about this the straight-forward solution would be to propose an amendment to 18 U.S.C. § 794(b) to eliminate the restriction of its effect to "time of war".)

Thus, I am back to the possibility that the real motive is not any one of those that have been put forward.

Whatever the motive for seeking the noncriminal standard, its implications are clear and disturbing. The fundamental issue is whether the Government has the right to conduct any form of surveillance of an American citizen whose conduct is not believed to be in violation of the law. Americans should be free to carry on activity which Congress has not made illegal without the presence of Government agents.

Moreover, once the principle of limiting th FBI to criminal investigations is breached, it is impossible to develop an effective check on the activities of the Bureau. Attorney General Stone put the matter clearly after the last great scandals of the Bureau of Investigation:

> The Bureau of Investigation is not concerned with political or other opinions of individuals. It is concerned only with their conduct and then only with such conduct as is forbidden by the laws of the United States. When a police system passes beyond these limits, it is dangerous to the proper administration of justice and to human liberty.

We should not lightly ignore that advice. The Government should be held to a very heavy burden of proof before Congress grants authority for an investigation under a noncriminal standard. The administration should be required to show not just that the added flexibility might be useful in some circumstances but that it is of great importance in significant cases. Thus far, it has failed even to demonstrate that there are cases where a noncriminal standard is even necessary. For the Congress, as its first act to control the intelligence agencies, to authorize electronic surveillance under these circumstances would, in my view, be an abdication of responsibility.

INDEXING OF INFORMATION

I must confess to being greatly perplexed about the lack of interest in the indexing of information gained from national security wiretaps under the names of American citizens.

Some of the most serious abuses of which we are aware have stemmed from the use of material gleaned from embassy wiretaps about the political activities of Americans. In the late 1960's when President Lyndon Johnson asked the Bureau what it knew about the anti-war views and activities of members of Congress, FBI Director J. Edgar Hoover turned to his richest source—embassy wiretaps—and began providing the White House with regular reports on the anti-war activities of Senator William Fulbright and other leaders of the movement to force an American withdrawal from Vietnam. (See Church Committee Report, Vol. III, pp. 313 ff.).

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Embassy wiretaps are also used to trace the contacts and activities of journalists. We know most about this practice from the file on Richard Dudman, the distinguished head of the Washington Bureau of the St. Louis Post Dispatch. Dudman has obtained much of his file as a result of a Freedom of Information Act request and subsequent lawsuit. The Bureau overheard Dudman numerous times on embassy wiretaps. These logs were often placed in Dudman's file or indexed so that they could be retrieved by a search for information about him. They were used by the FBI to develop a portrait of Dudman's activities and to assess the possibility of recruiting him as an agent. There is no reason to think that this is an atypical case.

S. 1566 not only does not prohibit such activity, but it actually, by omission and implication, sanctions it. The bill's procedures to minimize overhearing or recording conversations of people who are not the target of the tap apply only to information that does not relate inter alia to the ability of the United States to "provide for the national defense or security of the Nation" or "to provide for the conduct of the foreign affairs of the United States." With one exception, there is no requirement to even try to minimize the acquisition or retention of information within those categories even if it is obtained from United States citizens and relates to their views and activities.

The one exception is the prohibition on storing information relating "solely to the conduct of foreign affairs" so that it can be retrieved by reference to the name of an American. By implication, information (including people's opinions) related to national defense or national security can be stored so that it can be retrieved under the name of an American who was not the target of the surveillance and the bill provides no limitation on the use of such information.

I would urge this committee to include in the bill the amendment included in Mr. Shattuck's testimony that deals with this problem.

Mr. Chairman, I appreciate this opportunity to present my views on S. 1566. As one who has had the opportunity to read 21 months of FBI logs of his home telephones conversations, I inevitably bring to this subject a certain passion that others may not fully share. Surely, however, we all recognize the evil of unwarranted governmental intrusion and of the need to proceed with caution so that in our haste to reform we do not sow the seeds for later violation of our rights.

Point of View

"THE NEW WIRETAP REFORM BILL"

(By Morton H. Halperin)

Senator Edward Kennedy has recently introduced a revised national security wiretap bill, S. 1566, which has the support of the Carter administration and a bipartisan group of Congresspersons across a broad political spectrum. It is now very likely that, at long last, a bill will be passed to regulate electronic surveillance on national security grounds and to require a judicial warrant for all such surveillance, at least in the United States.

This seems, therefore, to be an appropriate time to step back and ask what the Foreign Intelligence Surveillance Act of 1977 (S. 1566) is all about. How well does it deal with the acknowledged abuses which have generated support for this legislation?

WIRETAPPING—PAST PRACTICE AND LEGAL HISTORY

To understand the purport of the proposed legislation one must examine practice and jucidial opinions both before and after the Supreme Court decision in 1967 putting wiretaps under the 4th amendment. Katz v. U.S., 389 U.S. 347. Electronic eavesdropping as a tool of espionage and counter-espionage has apparently been a part of the FBI investigative repertoire as long as the technology existed. Two diffeernt activities are at issue and the distinction is important to understanding the current draft of S. 1566.

One purpose of this national security surveillance is to gather information about the activities of foreign governments. There is no suggestion that illegal activity is underway; the State Department and the CIA simply want to know what is being said at the Russian and other key embassies. The ideal prototype is the lazy Russian Ambassador who routinely has emergency cables read to him at his mistress' residence because he does not want to come in to the Em-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

bassy in the middle of the night unless it is really urgent. Mostly, the fare is apparently much more meager; gossip and information about what people are doing which could, and perhaps sometimes even does, turn out to be of some use to the intelligence analysts.

The second type of "national security" surveillance which the FBI has traditionally conducted relates to the Bureau's counter-intelligence mission of keeping track of the agents of the KGB and other hostile intelligence services. In a typical case the surveillance moves from the foreign national to the American citizen suspected of being an agent. In most cases the Bureau's aim is to "turn" the agent or to pass false information; arrest and conviction are not usually the objectives.

Both of these activities were presumed by the FBI and the Justice Department to be beyond the control of the courts and not subject to the same Fourth Amendment limitations as other kinds of surveillance might be. Wiretapping has always been, to use Justice Brandeis' famous phrase, "a dirty business," but in the eyes of the Supreme Court it has only been covered by the Fourth Amendment since the Court issued the *Katz* decision in 1967. Thus, when the Supreme Court in *Irvine* (1954) condemned the use of microphones planted in a suspect's bedroom, the then Attorney General sent the following memorandum to the FBI:

> It is clear that in some instances the use of microphone surveillance is the only possible way of uncovering the activities of espionage agents, possible saboteurs, and subversive persons. In such instances I am of the opinion that the national interest requires that microphone surveillance be utilized by the Federal Bureau of Investigation. This use need not be limited to the development of evidence for prosecution. The FBI has an intelligence function in connection with internal security matters equally as important as the duty of developing evidence for presentation to the courts and the national security requires that the FBI be able to use microphone surveillance for the proper discharge of both of such functions. The Department of Justice approves the use of microphone surveillance by the FBI under these circumstances and for these purposes.

And when the courts held that Section 605 of the Federal Communications Act applied to government officials and prohibited the use of wiretap evidence in a criminal trial, the government interpreted the ruling to mean that it could continue to conduct electronic surveillance provided that the information obtained was not disclosed to anyone outside the executive branch.

The courts and the Congress were generally and vaguely aware of these practices but on the whole were prepared to leave the matter to the Executive Branch. There was then no evidence of abuse, for this was the pre-Vietnam/Watergate era in which it seemed appropriate to defer on national security matters to the President. And there was no constitutional issue since wiretapping had not yet been held to come under the protection provided by the Fourth Amendment.

THE FLAWS IN S. 1566

In tht late 1960s all of these conditions changed and controversy began to surround national security wiretapping. There is now a consensus on the need for legislation to control such surveillance and agreement now that all such surveillance should require a court order. To assess the adequacy of the current draft of S. 5166 it is necessary to carefully delineate what the abuses of the past have been and to determine if this legislation deals adequately with them.

WIRETAPS AND ILLEGAL EVIDENCE

The Supreme Court decision in *Katz* brought wiretaps under the Fourth Amendment for the first time and forced the Justice Department of Lyndon Johnson to take a closer look at FBI practices. The officials discovered that the FBI was routinely concealing the fact of wiretapping and other electronic surveillance from United States Attorneys and using the fruits of the surveillance to gather evidence for criminal convictions. The Justice Department began to admit to such wiretapping, particularly at the Supreme Court level, when the Solicitor General's office insisted on being informed of all wiretaps and on informing the Court of them.

The Court could no longer duck the issue of national security wiretaps and how they should be handled in a criminal case. In *Alderman* v. *U.S.*, 394 U.S.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4
93-179 O - 77 - 7

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

165 (1968), the Supreme Court held that the trial court must be notified of any overhearing of a criminal defendant on a wiretap. The court was then to determine if the surveillance was legal. If it was not, then the logs had to be turned over to the defendants for a taint hearing—to determine whether illegally obtained evidence was being used by the prosecution. The Court left open the questions of what kinds of surveillance violated the Constitution and what procedures the courts should use to determine legality.

S. 1566 seems to be attempting a step backward from the procedure mandate by *Alderman* to prevent the fruits of an illegal surveillance from being used in a criminal prosecution. Under tht provisions of the bill, if the court finds a surveillance illegal, it must surpress the evidence obtained from the surveillance, but it is not obliged to turn the illegal logs over to the defendants so that they can attempt to prove that other evidence introduced at the trial was tainted by illegal surveillance. This provision of the bill lays out a procedure to be followed "not withstanding any other law," which is apparently an attempt to set aside tht procedures which Congress passed to implement and in part to limit, the *Alderman* decision. S. 1566 also attempts to provide guidance to the court in how to go about determining if the surveillance is legal. In doing so, it emphasizes *ex parte in camera* proceedings rather than an adversary process.

OVERHEARING PEOPLE WHO ARE NOT THE SUBJECT OF THE TAP

A second abuse of the national security wiretap process arose from the use of information obtained from a surveillance placed on an embassy or other foreign establishment for the purpose of gathering foreign intelligence information. Embassy employees assume that their phones are tapped and generally proceed accordingly but many American citizens out of naiveté or necessity discuss business with foreign embassies over the telephone. Embassy taps thus produce significant information about the political views and activities of Congresspersons, journalists, and private citizens whose political or business activities brings them into contact with embassies.

The FBI has always, and continues to this day, to systematically exploit such information. In the late 1960s when President Lyndon Johnson asked the Bureau what it knew about the anti-war views and activities of members of Congress, FBI Director J. Edgar Hoover turned to his richest source—embassy wiretaps—and began providing the White House with regular reports on the anti-war activities of Senator William Fulbright and other leaders of the movement to force an American withdrawal from Vietnam.

Embassy wiretaps are also used to trace the contacts and activities of journalists. We know most about this practice from the file on Richard Dudman, the distinguished head of the Washington bureau of the St. Louis Post Dispatch. Dudman has obtained much of his file as a result of a Freedom of Information Act request and subsequent lawsuit. The Bureau overheard Dudman numerous times on embassy wiretaps. These logs were often placed in Dudman's files or indexed so that they could be retrieved by a search for information about him. They were used by the FBI to develop a portrait of Dudman's activities and to assess the possibility of recruiting him as an agent. There is no reason to think that this is an atypical case.

Incredible as it may seem, S. 1566 not only does not prohibit such activity, but it actually, by omission and implication, sanctions it. The bill's procedures to minimize overhearing or recording conversations of people who are not the target of the tap apply only to information that does not relate *inter alia* to the ability of the United States to "provide for the national defense or security of the Nation" or "to provide for the conduct of the foreign affairs of the United States." With one exception there is no requirement to even try to minimize the acquisition or retention of information within those categories even if it is obtained from United States citizens and relates to their views and activities.

The one exception is the prohibition on storing information relating "solely to the conduct of foreign affairs" so that it can be retrieved by reference to the name of an American. By implication, information (including people's opinions) related to national defense or national security can be stored so that it can be retrieved under the name of an American who was not the target of the surveillance and the bill provides no limitation on the use of such information.

The failure to deal with this problem cannot be explained by the fact that no one has focused on it. The American Civil Liberties Union has been urging the adoption of an amendment which would need read as follows:

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Information obtained under the procedures of this chapter from a United States person who is not the target of surveillance shall not be maintained in such a manner as to permit its retrieval by the name of that person unless it is: (a) evidence of a crime; (b) evidence that the person is a foreign agent eligible for surveillance; and (c) in a file maintained solely to respond to court orders related to electronic surveillance.

Unless something along these lines is added to the bill, its enactment will sanction one of the worst and best documented abuses of national security wiretapping.

SELECTION OF TARGETS

Another set of abuses arises from the question of who should be tapped on national security grounds. Originally such surveillance appears to have been limited to the tapping of embassies to gather foreign intelligence and to the surveillance of those believed actually to be spies in the service of the KGB. Gradually, however, the scope of the surveillance expanded to include men such as Martin Luther King, Jr., who were asserted to be in contact with American communists and in danger of being controlled by them. Under the Nixon Administration, there were two expansions of the categories of people on which electronic surveillance might be conducted. One was secret and relatively small—the taps ostensibly intended to track down leaks and placed on newspapermen and government officials. The other was publicly proclaimed and massive.

The public program stemmed from the assertion by Attorney General Mitchell that he could authorize the surveillance of American citizens who were not believed to be in the service of a foreign power but whose activities were believed to pose a threat to "internal security." Under this program elements of the anti-war movement were surveilled, as were organizations including the Jewish Defense League and the Black Panther Party.

When members of these organizations were indicted, they demanded access to electronic surveillance logs thus requiring the courts to rule on the legality of various forms of electronic surveillance. With a few minor exceptions the courts have held that warrantless taps of embassies are constitutional, but that warrantless taps directed against American citizens who are not connected with a foreign power are unconstitutional. No court appears to have been confronted since 1968 with a surveillance targeted on an American citizen, who, it was claimed, was an agent of a foreign power.

The Supreme Court considered the matter only once in a case involving a group without any connections with a foreign power. In what has come to be known as the *Keith* case (after the District Court judge whose opinion was upheld) the Court ruled tat the President did not have the power to conduct warrantless electronic surveillance of domestic groups. The court, however, went on to indicate that Congress could authorize warrants for electronic surveillance for domestic intelligence purposes on a standard other than probable cause to believe that a crime was being committed. *U.S.* v. *U.S. District Court*, 407 U.S. 297 (1972).

Perhaps the most important thing about S. 1566 is that it does not pick up this invitation, and instead makes it clear that the executive and the judiciary should not together fashion a warrant standard for such domestic intelligence surveillance. With the enactment of this legislation, it will be clear that a person whom the government does not charge with being an agent of a foreign power may not be surveilled electronically except with a warrant based on probable cause to believe that a crime has been or is about to be committeed and that evidence of the crime will be gathered.

WHO IS AN AGENT OF A FOREIGN POWER?

The remaining and troublesome question has to do with the standard under which the government can bring a citizen or other person under the purview of the agent-of-a-foreign-power standard. Much of the debate on this question has forcused on the important question of the so-called non-criminal standard but there is a broader question of how clearly the legislation defines the circumstances in which an individual may be surveilled on suspicion of being an agent of a foreign power. Regrettably, the current bill takes several steps backward from S. 3197, the bill reported last year by the Senate Intelligence Committee.

The retrogression, which appears to be the deliberate work of the intelligence agency professionals (who reportedly were given a greater role in this effort)

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

relates to (1) the category of "non-U.S. persons," (2) the vague criminal standard to which a more vague conspiracy clause has now been added, and (3) the non-criminal standard paragraph which is a bit more vague than S. 3197 and to which for the first time has been added a conspiracy clause which renders its safegards irrelevant.[1]

S. 1566 creates a new category of persons who may now be wiretapped. People who are lawfully resident aliens can be wiretapped if they are engaged in something called "clandestine intelligence activities" (which is nowhere defined—see discussion below) in a manner which indicates that the activity would be harmful to American security. This open-ended authority is essentially the standard contained in S. 3197 as it was reported by the Senate Judiciary Committee and which the hearings of the Senate Intelligence Committee showed were ambiguous and full of loopholes. Visitors to our shores—whether simple tourists, lecturers, students or businessmen—are to be subjected to surveillance under far less stringent conditions than citizens; both the wording of the Fourth Amendment, which applies to all "persons" and the spirit of our system which has always been to accord all of the protections of the Constitution to all of those lawfully within our borders, would be ignored. No case has yet been made for the need for this major expansion of S. 3197.

The second set of problems relates to the paragraph which authorizes surveillance of a person who: "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."

That paragraph does not represent any change from S. 3197, but in the flurry of controversy over the non-criminal standard it has never gotten the careful scrutiny it deserves: "Clandestine intelligence activity" is not defined. Nor is there a list of the crimes which would give rise to the possibility of electronic surveillance. Removing those two defects would provide precision and fair notice of what conduct might subject one to such surveillance. Retaining them leaves broad loopholes.

The conspiracy provision which goes with this section has been re-written without the administration's having called the changes specifically to the attention of the Senate staffers working on the bill. It now provides that one need only conspire with or knowingly aid or abet any person engaged in such activity; unlike the earlier S. 3197 version, it does not require that the conspirator know the nature of the activity engaged in by the person being aided.

This conspiracy provision also now applies to the non-criminal standard paragraph. This is a major change and an enormous step away from narrowing the scope of the non-criminal provision. As it finally emerged from the Senate Intelligence Committee last year, the non-criminal standard section had no conspiracy provision at all. The individual to be surveilled had to be a knowing member of an intelligence network, transmitting information at its direction. The conspiracy clause throws the net over those who can be said to be assisting such an agent even if they do not know what the agent is up to. There are also a number of seemingly minor drafting changes in the paragraph which add up to a significantly looser standard.

Senate aides have suggested that the intent was to return to the language of S. 3197 as ultimately revised, and that that will be done by the Judiciary Committee after its hearings in the middle of June.

TARGETING PEOPLE NOT SUSPECTED OF CRIME

Even so, it would still leave the fundamental question of whether individuals who are not suspected of criminal activity should be the subject of electronic surveillance.

As Senator Kennedy noted in his statement announcing his intention of introducing the administration bill, the Justice Department has never made it clear why it needed a non-criminal standard.

Originally it was claimed that the provision was needed because the espionage law does not cover industrial information. However, when it was pointed out that the Supreme Court in interpreting the phrase "national defense" in which the *Gorin* case had given it a very broad meaning which clearly included indus-

[1] Those concerned with embassy taps have also seen that the bill is now written so that such taps can be authorized (1) by the Assistant Attorney, (2) for a period of up to one year, and (3) without requiring that the court be told exactly how the surveillance will be effected, whether by burglary or other means. These are major changes.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

trial information, this explanation was abandoned. The original draft from the Bell Justice Department expanded the definition to include harm to foreign affairs (which is not covered by the espionage law), but this expansion has now been abandoned in the bill as introduced. S. 1566 does expand the activity covered to include collection as well as transmittal of information. However, if the collection was with a view towards transmittal it would be covered by the conspiracy provisions. If collection really is the problem, then it could be cured by proposing a simple amendment to the espionage laws to make the collection of protected information by an agent of a foreign power a crime in peacetime as well as in wartime. We could then debate that proposed change in the criminal law.

One suspects that the motives of the intelligence agencies, notably the FBI, for wanting a non-criminal standard for investigations is the same as the reason why those who have opposed the non-criminal standard are concerned: this legislation will cast a shadow over so-called counter-intelligence (i.e., political) investigations of the FBI.

Operating under secret guidelines promulgated by Attorney General Levi, the FBI currently conducts counter-intelligence investigations of American citizens under a very loose and non-criminal standard which is reported to be very close to the standard in the original Levi version of S. 3197. That standard would permit surveillance of a large number of American citizens who are suspected—if only because they are dissidents—of relating in some way to a foreign power. By authorizing electronic surveillance under some circumstances without suspicion of crime, the legislation would be taken by the Bureau as constituting authority to conduct "lesser" forms of surveillance, including the use of informants (which is not currently held to fall under Fourth Amendment standards) under much looser standards. Such surveillance can then be used to establish whether a warrant for a wiretap can be obtained.

As Attorney General Harlan Fiske Stone warned long ago, and as the Church Committee reminded us recently, departing from a criminal standard opens Pandora's box. With the Church Committee and others documenting numerous cases of abuse stemming from a departure from the criminal standard it would be more than ironic if the first piece of legislation enacted by the Congress in response to the scandals were to ignore Stone's prophetic warning:

"The Bureau of Investigation is not concerned with political or other opinions of individuals. It is concerned only with their conduct and then only with such conduct as is forbiden by the laws of the United States. When a police system passes beyond these limits, it is dangerous to the proper administration of justice and to human liberty."

No bill which ignores that warning can be said to be effectively dealing with the abuses of the past.

Senator KENNEDY. You have been very helpful.

Many of these areas obviously are troublesome to us and the members of the committee. We pursued some of them in the exchange yesterday. We continue to be concerned about them.

As far as I am concerned, we ought to clearly understand in the establishing of any future FBI charter that we are not establishing precedences here in this legislation for the charter.

S. 1566 focuses on a problem which exists today and has existed for a number of years. The charter is a completely different issue. However, we must fashion and shape an FBI charter. That is a very basic and fundamental goal and we must get a positive reaction and response from the administration.

I do not feel that we are endangering in any way what the criteria will be to guide the Bureau in the area of charter reform by the actions that we take today with S. 1566. We differ, but at least that is my viewpoint.

The inherent power provision which has been eliminated I think has been a very significant and important improvement in this legislation. I think that that is no small achievement. I think that shows important progress in this whole area. I expect you to agree with that.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Mr. HALPERIN. I think there has been some progress in this area, but I think it is important to understand that there is still an inherent power provision in this bill. It appears on page 28, line 12.

What it basically says as I read it is that the activities of the National Security Agency in intercepting telegrams entering and leaving the United States provided they do not target the name of an American citizen are neither authorized nor unauthorized by this bill. That activity is left in exactly the same place.

I do not know that there is anything more than can be done in this bill about that.

As I read the bill, the National Security Agency could put the word "terrorism" into its computer and then read every cable that mentions the word "terrorism," whether it is addressed to an American citizen or from an American citizen even if it is from one American citizen to another American citizen, provided one of them is outside the United States.

The bill simply says, again, if the President has authority to do it, he can do it, and if he does not have authority to do it, he cannot do it.

Senator KENNEDY. Do you mean with regard to the provisions that apply to the Intelligence Agency in meeting the challenge of counterintelligence?

Mr. HALPERIN. No. The provision beginning on line 12 has to do with the National Security Agency, as I read it, to affect the acquisition by the U.S. Government of foreign intelligence information from international communications by a means, other than electronic surveillance.

Senator KENNEDY. That is the overseas problem.

Mr. HALPERIN. No; it is not. A person can be in the United States. If you are in the United States and you send a cable, the only part of that that is covered is the business that we talked about this morning of known U.S. persons.

The definition of electronic surveillance on page 6, beginning on line 15(a) is acquisition of radio wire communications that go overseas only if sent or received by a particular known U.S. person.

If they are intercepting every cable that moves over a wire, say, between New York and London——

Senator KENNEDY. We are concerned about that. I am hopeful we can get together with Senator Bayh and the others. You are pointing out an area that is a matter of concern for us.

Mr. HALPERIN. This is not overseas. This is somebody in the United States.

Senator KENNEDY. Sending overseas?

Mr. HALPERIN. Sending overseas.

Senator KENNEDY. Comparing that with the inherent power deletion is a dramatic contrast in terms of magnitude and importance.

Mr. HALPERIN. I agree. I agree. All I meant to say—and it really is a footnote—is that there is an area in which Congress is again simply saying if the President has the authority he can do it and, if he does not have the authority, he cannot do it. However, I did not mean to blow that out of proportion.

I think there has been a substantial reduction in the Presidential power.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Senator KENNEDY. Are we better off with this bill or with the current situation without this bills protections, given the fact that we have gone 7 years without the opportunity to get any legislation at all?

Mr. Shattuck?

Mr. SHATTUCK. Senator, I think the real thrust of our testimony on the fourth amendment and the crime standard is that whatever the practices may be—and we are finding again and again that there are abusive practices with respect to wiretapping—the law is remarkably clear on our side. By "our side," I mean the side that says no wiretaps at all without probable cause to believe that a crime has been committed.

There are only a scattered number of court of appeals decisions and District Court decisions that even raise the possibility of a foreign security exception to the warrant requirement on the criminal standard. There is no Supreme Court decision.

I think whatever one's view of the Supreme Court today might be, and I understand that various people might differ about this, how the Supreme Court would come down on cases like this, looking at the law as it now is I do not regard this bill—to the extent that it permits wiretaps on American citizens and, secondarily, foreigners, but principally American citizens, without probable cause to believe that they are engaged in crime—as an advance over existing law.

That is a reading of the law that you will find in our statement. We recognize that the few decisions that go the other way are court of appeals decisions in the foreign security area.

Senator KENNEDY. Do you think we ought to wait until the Burger court makes a decision on this?

Mr. SHATTUCK. No; that is not what I am suggesting. The ball is now in the court of Congress. I think the opportunity is enormous for bringing the law of wiretapping into conformity with general fourth amendment law as I have outlined it.

I think that were the law to be taken in that direction so that the crime standard would apply at the very least for American citizens, then there would be an improvement over existing law. There is no question about it.

As the bill now stands, however, we have strong reservations about it. In fact, as I have suggested in my testimony, we do not regard it as a substantial improvement.

Mr. HALPERIN. It seems to me that this committee could easily take the position that the administration has not met the very heavy burden of saying there should be a noncriminal standard and report a bill which eliminates the wiretapping of American citizens to a criminal standard.

That would still give the Justice Department the opportunity——

Senator KENNEDY. That is completely unrealistic in terms of the makeup of the committee.

I think you have a consistent position if you want to say that your positions are going to be upheld by the Burger court and, therefore, you are willing to wait until those matters are raised and you think you will get a stronger standard when the Burger court acts.

However, I believe it is completely unrealistic to think that you are going to get that standard in the form of Senate legislation.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

I respect your view as an interpreter, but you also have to look at the particular attitude and sincere views that are held by others in the Congress. They do not happen to be mine, but they do exist.

Mr. HALPERIN. Senator, I certainly would not want to give you advice about the Judiciary Committee. I understand there is a problem. The alternative obviously is to vote to report the bill but to make it clear that on the Senate floor you intend to introduce an amendment which would limit it to a criminal standard. If we lose that on the floor, then there is a harder problem.

If it is clear that the Congress will not vote the bill limiting it to a criminal standard, then I think the case to say "this is the best we can get so let's get it" becomes very strong.

I certainly think that the issue should be fully aired in this committee and in the Intelligence Committee and that there should be an effort on the floor to see whether a majority can be mustered for that position.

Mr. SHATTUCK. Senator, may I just add one comment to that?

Senator KENNEDY. Certainly.

Mr. SHATTUCK. I would like to clarify some of the points we were making earlier.

I do think that if this committee were to adopt this bill and Congress were to adopt it, it would very much be the first step in the whole control of the intelligence agencies legislation. The problem is that the control would not, we think, be very strong if there would be a noncriminal standard and a great deal would be lost, certainly with respect to the investigation of American citizens.

I think there is an issue here. There is a tug of war. There is a tug of war—no question about it—between the intelligence agencies and the Congress and perhaps even the intelligence agencies and the President. I do not think that one side should yield on that tug of war on the grounds of expediency. This is a very delicate and important and far-reaching matter. If we do not establish the right standards in this bill, it will be very difficult to proceed further.

I am sensitive to what you said, Senator, with respect to the fact that this legislation has a long history and has proceeded on a separate track. It also is coming at the time when intelligence control is of paramount importance.

Senator KENNEDY. I think these concerns are terribly, terribly important. They are troublesome to me and other members of the committee.

I do think in striking a balance that the elimination of the inherent power provision is crucial. We are not dealing with the overseas problems or the kinds of problems that Mr. Halperin mentioned but we are dealing with an inherent power justification which has been utilized and abused in recent history, and which still exists at the present time and will continue to exist until this statute becomes law.

That poses dangers for the future. That exists today. It existed yesterday. There is nobody who understands it better than Mr. Halperin and others. Inherent power has been restricted and effectively eliminated in this legislation.

With the passage of this legislation, even under the standards which have been included in the noncriminal application procedure, you will not have that abusive situation again.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

You can say, "Well, there are still troublesome aspects to it." I agree, these are troublesome to me as well.

The question is, I think, whether in the final analysis we are making important progress in the protection of the liberties of the American people.

I am troubled by the areas which you have mentioned here. However, it seems to me we may be able to make some progress at last. I've been trying for 7 years. Maybe we can get this legislation enacted. We have every intention of attempting to do it.

Without this legislation, you continue to leave open the opportunity for the serious abuses which we have seen in the past. There is nothing other than the intention, the goodwill, and the disposition of an executive that would restrict the possibility of abuse.

In striking a balance, I am not prepared to see that discretion continue.

Mr. HALPERIN. Senator, may I comment?

Senator KENNEDY. Yes.

Mr. HALPERIN. I think we all very much appreciate what you have been trying to do in this area. There obviously is a lot of force to what you are saying.

I think we also have the feeling we are still in a bargaining situation. The question of ultimately what is better than nothing is a position that I think one has to reserve when negotiations are still going on about changes.

I think the notion that it is important to get regulations and restrictions in this area is one at least that I personally am very sensitive to.

On this question of the special category of non-U.S. persons, if I heard what Mr. Kelley was saying yesterday correctly, he is mainly concerned particularly with the Soviet Union and with the fact that there are large numbers of Soviet seamen and students.

In answer to your question of why he needed this, he read out just Soviet numbers.

If, in fact, the concern of the Bureau is limited basically to the Soviet Union and some countries that are associated with it, it may be possible both in the drafting of the provision and in the language that accompanies it to make it clear that it is intended to be used simply for that limited category of countries, maybe even by saying that. However, if there is a diplomatic objection to that, then the language can be drafted that way.

As the language is now written, it would permit Iranian students, visitors from the United Kingdom, and all sorts of other people to be open to this abuse.

Nobody would be troubled by the notion that Soviet students are, in fact, employees of the Soviet Government in many cases. The same thing is true of Soviet seamen.

I think if that is, in fact, all of the concern, it may be possible to draft language there that covers that issue without seeming to open it up to every person who happens to be in the United States if not a permanent resident or alien.

Senator KENNEDY. We will look forward to examining your full statements in detail. It has been very helpful to hear your comments on this. Thank you very much.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Mr. HALPERIN. Thank you, Senator.

Mr. SHATTUCK. Thank you.

Senator KENNEDY. Our next witnesses will be Ms. Esther Herst, Committee against Repressive Legislation; Prof. William Greenhalgh, Law Center, Georgetown University; and David Watters, on behalf of the American Privacy Foundation.

Will you all come up as a panel, please?

Ms. Herst, you may proceed.

STATEMENT OF ESTHER HERST, NATIONAL COMMITTEE AGAINST REPRESSIVE LEGISLATION

Ms. HERST. Thank you.

Mr. Chairman, I am pleased to have the opportunity to testify before this subcommittee on the subject of S. 1566.

Senator KENNEDY. Your statement will be printed in its entirety in the record.

Ms. HERST. Thank you very much.

[Material follows:]

PREPARED STATEMENT OF ESTHER HERST, NATIONAL COMMITTEE AGAINST REPRESSIVE LEGISLATION

Mr. Chairman, I am pleased to have the opportunity to testify before this Subcommittee on the subject of S 1566, the Foreign Intelligence Surveillance Act of 1977. I am Esther Herst, the Washington Coordinator of the National Committee Against Repressive Legislation. NCARL is a citizens education-action organization which focuses primarily on the defeat or repeal of legislation which we believe threatens the basic First Amendment rights of free speech, press, and association. For most of our 18 year existence, we have worked to raise public consciousness of the Bill of Rights, what it means and how to protect it. We view our opposition to S 1566, as presently drafted, as one part of our program to stop abuses of Constitutional rights by intelligence-gathering agencies.

Our concern about S 1566 is grounded in the reality of FBI-CIA and executive branch excesses which have been so extensively documented by the Senate and House Select Committees on Intelligence, the Rockefeller Commission, and numerous press exposes. These investigations have confirmed what, for so long, we have feared: that the federal agencies charged with law enforcement and the protection of our national security have, in fact, been engaged in illegal, unconstitutional, and dangerously repressive activities. These activities have disrupted the constitutionally protected actions of thosuands of American citizens and have chilled the rights of countless others—bringing us closer than we dare come to a society run by secret police agencies.

NCARL is opposed to S 1566 initially because of our opposition to any and all electronic surveillance. Wiretapping and bugging are among the most intrusive means of finding out what people think, say, and do. While a warrant requirement may "control" the number and types of bugs used, the fact remains that any electronic surveillance constitutes a general search in our opinion and is, therefore, in conflict with the Fourth Amendment. We support a complete halt to federal or local wiretapping authority, for either criminal investigations or intelligence gathering.

S 1566 would give the first legislative sanction to wiretapping solely for the purposes of gathering information. While the country's security can quite adequately be protected against espionage, treason, or sabotage by the present criminal investigative wiretapping laws, S 1566 would give new and specific authorization to the government to listen for information totally unrelated to criminal activity but which allegedly fills some undisclosed intelligence needs. While it purports to control one of the most abominable of the intelligence abuses, "national security" wiretapping, S 1566 would, in fact, legitimize the rationale behind that abuse. The broad definitions in S 1566 for "foreign power," "agent

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

of a foreign power," and "foreign intelligence information," and the use of undefinted terms, such as "clandestine intelligence activities," will leave intact the concept that political dissenters, and especially those with an alleged foreign connection, are subject to government surveillance on the basis of constitutional political beliefs. We would remind the committee that most of the political surveillance and disruption in recent years was rationalized by a search for this elusive "foreign domination."

Government spying on individuals and organizations for political ideas is precisely the kind of activity that must be stopped and S 1566 does not attack that problem effectively. NCARL shares the concerns expressed by both Sen. Kennedy and Sen. Bayh about the use of a "non-criminal" standard in S 1506 and we wholeheartedly endorse the statements of the ACLU and Morton Halperin. Not only will the lack of a stringent criminal standard effect the use of politically motivated wiretaps but it will establish a frightening legislative precedent that could be followed by legislation authorizing mail-covers, informants, and the use of other surveillance techniques for non-criminal purposes.

NCARL finds it strange and disheartening that the first piece of legislation likely to be passed since the revelations of massive law-breaking by intelligence agencies should be a bill that would allow invasions of personal privacy, albeit with increased procedural and reporting requirements. While we applaud any meaningful effort to limit the use of electronic surveillance, we do not believe S 1566 represents such an effort.

Besides the non-criminal standard used in the bill to authorize wiretaps on American citizens and others, we have strong objections to the special dategory of people established by the bill: those who are not U.S. citizens or permanent resident aliens. Such a category includes foreign visitors, tourists, journalists, academics, students, and others who work here at the behest of a "foreign power." The creation of this special class codifies a notion that has long plagued our nation: that somehow non-resident aliens do not qualify as "people" when the Constitution guarantees "people" certain rights and protections. Coupling the non-criminal standard with the conspiracy clause that is applicable to these "non-people" leaves foreign visitors open to surveillance and spying by a government that purports to be a free and open democracy.

Another target for surveillance under the expansive definition of "foreign power" is embassies and, while we understand that intelligence agencies feel it necessary to bug foreign missions, we do not see how such bugging can be allowed under the present state of international law. We refer specifically to the Vienna Convention on Diplomatic Relations, signed by the President in 1972, with states that "the premises of the mission, their furnishings and other property thereon * * * shall be immune from search, requisition, attachment or execution." Surely the Committee is aware that the information gathered from embassy taps may be planted or simply gossip. Also, wiretapping embassies means overhearing thousands of conversations with American citizens. We therefore question the need for such surveillance, especially when carried out with such inadequate safeguards against abuse and for such long periods of time (up to one year) as are mandated by S 1566.

Procedurally, S. 1566 contains severe deficiencies. The same problems that were raised in regard to S. 3197 are applicable to this new bill as concerns the choices of seven judges and the Justice Department decision about which judge to approach with a warrant application. Since there are no guidelines as to qualifications, time of service, or reason for removal of these judges, the possibility remains for judges to serve so long in their capacity that they begin to view themselves as part of the intelligence establishment. Conversely, judges who reject too many Justice Department warrant requests can be relieved of this special duty. The Justice Department may go to any of the seven judges, allowing them the option of consistently choosing whichever judges will be most sympathetic to their application.

The review procedure, while an improvement over S 3197, is still grossly inadequate. The illusion of impartial judicial review is perpetuated by the limitations of the certification procedure. Although the judge must find that there is probable cause to believe that the target is a foreign power, he does not have the opportunity to determine if there is, in fact, a need for the information being sought; that it will, in fact, be heard over the surveilled conversations; or that the value of the information outweighs the privacy guarantees of the Constitution. The judge can decide that the certification is "clearly erroneous"

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

in the case of American citizens, but that standard is almost laughable given the ex parte nature of the hearing. We would recommend instead that the judge find probable cause to believe that the certification is correct and we would urge that the judge have the opportunity to look behind the certification in all cases (not only U.S. persons) in a much more meaningful way.

The protections given by S 1566 to persons being overheard by government authorized electronic surveillance are unacceptable. The minimization procedures should apply to all those overheard, not only U.S. persons. Also, the expungement of information required in S 3197 should certainly be included in these minimization procedures. NCARL supports Morton Halperin's recommendation that U.S. persons be protected against the storage of foreign intelligence information even if it is not related solely to the conduct of foreign affairs.

NCARL is deeply concerned about the notification provisions of S. 1566. We believe that the bill presently is very unclear about the need for an adversary hearing before information gathered from a national security tap can be used as evidence in a criminal case. It is hard to understand how defendants or "persons aggrieved" can be protected against government illegality when they are not even allowed to participate in the hearing which determines the legality of the surveillance.

We are also concerned that the simple suppression of evidence gathered illegally is not sufficient protection for the defendant and we would urge that, when the court determines or the government concedes that the surveillance was illegal, the logs of the surveillance be turned over to the aggrieved person so that they can be challenged for taint. Additionally, we feel very strongly that the government must inform all people, not only U.S. persons, when an emergency tap has been placed and a warrant is not subsequently issued.

There is a policy question to be considered in the area of notification. If the information gleaned from a national security tap is to be used in a criminal proceeding, should not the requirements of Chapter 119 be followed instead? Or, if the surveillance authorized by S. 1566 is for information-gathering purposes, only, should not an even heavier burden of proof and protection be imposed upon the government when it wishes to use such information in a criminal case? S. 1566 does not adequately resolve this dilemma.

The provision requiring that landlords, custodians, and others cooperate forthwith with the government in the placing of a national security tap or bug conjures up images of totalitarian states which force citizens to participate in spying activities against other citizens. This section should certainly be changed to make the cooperation optional, lessening the Big Brother spectre it raises.

While we are glad to see that citizens and permanent resident aliens may sue the government when a violation of this legislation occurs, we are distressed by the prohibition on such suits by foreign visitors, that special category of non-people established by S. 1566. Since one purpose of allowing civil suits is to deter illegal taps, this provision would seem to sanction illegal surveillance on aliens, who will have no redress against the government.

Finally, S. 1566 leaves several loopholes through which intelligence agencies will be able to invade the privacy of innocent people and carry on unconstitutional political surveillance. The provisions which allow for unwarranted wiretaps of up to 90 days to test equipment capability are not in keeping with the bill's alleged purpose of halting unauthorized electronic surveillance. The agencies have never publicly documented why such a provision is needed and, due to the bill's requirement that the tapes of these "test taps" be destroyed, there is no opportunity for Congressional oversight. S. 1566 is even worse than S. 3197 was in that it allows for unwarranted and unlimited taps to determine if electronic surveillance equipment is being used unlawfully. Here, again, there has been no showing that warrantless taps are needed for this purpose and the potential for abuse is obvious.

Senator Bayh has noted that S. 1566 does not extend any protection to Americans outside of the United States. While the controls placed on taps originating within the U.S. are an improvement over S. 3197, the silence about surveillance of Americans abroad is dangerous. In effect the bill continues the possibility of a presidential claim of "inherent power" to wiretap abroad without judicial review or controls of any kind. NCARL recommends that clear privacy protections be extended to Americans outside of the U.S.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

We are deeply concerned about the inadequate congressional oversight mandated by S. 1566. We object to the weak oversight provisions of S. 3197 and S. 1566 is even less satisfactory in that respect. Certainly, at the very least, there should be an inclusion of the review requirements of S. 3197. Preferably, S. 1566 should be amended to include congressional access to information describing the benefits to U.S. interests derived from national security electronic surveillance. We would caution, however, that the reports to Congress must be made with due consideration for the privacy of innocent individuals and organizations overheard.

For all of these reasons, we hope that this committee will not report S. 1566. At a time when public confidence and trust in government are at a dismally low level, people are looking hopefully, though skeptically, for some signs of change—for some indication that Congress will take meaningful and positive steps to end the many violations of our rights by intelligence agencies. Passage of S. 1566, with all its loopholes and pitfalls, can be seen as a step towards legitimating the abuses, rather than preventing them. It can be seen as a frightening example of how little Congress has learned about the abuses of power of the last quarter-century. Similarly, passage of S. 1566 can be seen as a capitulation to the philosophy that the interests of "national security" must take precedence over the protection of human rights and that needs of the intelligence agencies are more important that the democratic principles mandated by the Constitution and the Bill of Rights. We hope that this committee will not allow such a capitulation to occur and will, instead, reaffirm your commitment to due process and freedom of thought in our society by defeating S. 1566.

Senator KENNEDY. We are having an important hearing on S. 270, which is the intervenor legislation, of which I am the prime sponsor, up in another room. This is terribly important, too.

We will put all of the statements in the record. If you could summarize your statement, then I will have some questions for you.

Ms. HERST. Our testimony is based on the reality of CIA, FBI, and other intelligence agency abuse about which we have learned in revelations over the past few years.

We are very concerned about any opportunity to authorize continued political surveillance of American citizens or people within the United States on grounds of their political beliefs. We see that S. 1566 would continue such authorization.

We are concerned certainly about the same things that Mr. John Shattuck of the American Civil Liberties Union spoke about as well as those concerns expressed by Mr. Halperin.

The National Committee against Repressive Legislation is opposed to all wire tapping as in conflict with the 4th amendment.

We are also opposed to the very broad definitions within S. 1566, specifically as they refer to foreign powers, agents of a foreign power, foreign intelligence information, and the undefined clandestine intelligence activities.

We are concerned about the noncriminal standard as it applies to American citizens and resident aliens.

The special category of foreign visitors, I would again reemphasize what Mr. Shattuck and Mr. Halperin had to say about that.

Our statement goes into some detail about the procedures for the judicial review, the choosing of the seven judges, the ability to go behind national security certification in determining whether or not a tap or bug ought to be placed. We have some strong reservations about whether they, in fact, institute meaningful controls on national security agencies.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

We are also very disturbed by what we consider lack of protection of people who are overheard, the ability to challenge the illegality of the surveillance, the ability to get the logs so that they can be challenged in a criminal proceeding, and also the policy question of whether or not information that is gathered under this provision should be used at all in a criminal proceeding. If the information is going to be used in a criminal proceeding, perhaps the requirements of chapter 119 should apply instead.

Certainly the loopholes in terms of wire tapping abroad are of concern to us as well as the ability to wire tap without any court order for testing equipment capability or for determining whether electronic surveillance equipment is being used unlawfully.

We are also bothered by the lack of congressional oversight written into S. 1566. It is even less than was in S. 3197.

We would strongly recommend that you go through the amendments that Mr. Shattuck submitted and take serious time to look through them, and hopefully pass them.

Senator KENNEDY. Professor Greenhalgh, you may proceed.

STATEMENT OF WILLIAM W. GREENHALGH, PROFESSOR, LAW CENTER, GEORGETOWN UNIVERSITY

Mr. GREENHALGH. Mr. Chairman, I will just take a couple of minutes because I have submitted a 10-page statement with 35 Supreme Court cases, 3 English cases, and 1 case coming out of Massachusetts which started the precepts of the fourth amendment.

One thing that has not been brought to your attention during these 2 days of hearings concerns me greatly. That is the involvement of the Chief Justice of the United States in consultation with the Attorney General and the Director of the Central Intelligence Agency.

Mr. Chairman, there are three basic essential elements to the fourth amendment warrant requirement. One of those is neutrality an detachment of the issuing magistrate.

I think if you read very carefully *Shadwick* v. *the City of Tampa* you will see language in there: "There shall be no connection between the judiciary and law enforcement."

I do not think that is an essential part of the statute which is contained in 2523(c). In order to really protect the Chief Justice, Mr. Chairman, where will this case go ultimately if there is ever a prosecution? Or course, there will be a motion for recusal.

Second, 2526(c) is a blatant attempt by the United States Department of Justice to overrule *Alderman* v. *The United States*.

If we are to have pretrial screening in camera as well as ex parte, it flies in the face of that five to three decision in 1969. As existing law today, 2526(c) is unconstitutional, pure and simple.

For somebody not to tell you that, I think that would be in error.

Also the traditional probable cause test is lacking concerning clandestine intelligence activities, harmful to security, and so forth and so on.

They come back and tell you yesterday *Camara* v. *Municipal Court* will handle it; the *Keith* case will handle it; *Alemida-Sanchez* will handle it; and then they also talk about the *James* case.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

I disagree. I think in *Keith* you get some indication from Justice Powell if there is a legitimate need vis-a-vis protection of rights, then maybe the court will take a different view of it, but I do not think the Department has yet presented to this committee and to the U.S. Senate a standard by which it will pass constitutional muster, which is the second element, and that is probable cause.

Also, I would be very much concerned with the proposed noncriminal standard. It is void for vagueness under the fifth amendment.

See *Papachristou* v. *City of Jacksonville.*

If "car prowling" was thrown out, how about the word "clandestine"?

Last but not least, the other ingredient——

Senator KENNEDY. You do not think it is as clear as the espionage law; is that correct?

Mr. GREENHALGH. Senator, that is a simple answer. The Attorney General challenged you yesterday, "Give me a time limit." The simple answer is a comprehensive revised espionage law that should be put into this bill as soon as possible.

Senator KENNEDY. What about the current one?

Mr. GREENHALGH. Apparently they are tinkering with it.

Senator KENNEDY. I am talking about the existing one. I know they are redrafting it, but the existing one.

Mr. GREENHALGH. That throws it in but you know they are still having problems with definition of national security.

I do not see why with all of those lawyers down there that they cannot get something back up here in a couple of weeks. I really don't. They can turn that Criminal Division upside down. They can come back here with a piece of legislation. He challenged you yesterday. He said, "Give me a time limit." That is just a suggestion.

Last but not least, is the law of particularity. This is very, very important when you are dealing with the fourth amendment.

Senator, the provision provided in 2525(b)(1)(C) should have stronger language particularizing the type of information they are seeking not only on the application, but also in the order. This is very important.

As it is presently written, the 90-day—and God forbid, the 1-year—duration, it is a general warrant, pure and simple. It flies in the face of *Go-Bart*, *Marron*, *Stanford*, *Berger*, and *Stanley*—all of which I have cited in my statement.

It is too wide open. It is too imprecise. It is too indiscriminate. It sweeps everything.

Your minimization procedures cannot help it. Justice Tom Clark who wrote the *Berger* opinion, and who passed away yesterday, certainly made this very clear in the *Berger* case when he wrote it.

Sixty days was too long. What did you all do? You responded to that after the *Katz* case came down and put a 30-day limit in title III.

If the Department of Justice can almost get its act together within 24 hours, why in the world do they need 90 days?

I would suggest that you follow, especially to tighten this piece of legislation up, rule 41(c) of the Federal Rules of Procedure which provides for a 10-day execution, and also the decision of *Sgro* v. *United States*, as cited by the Supreme Court, I believe, in 1932.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

The Administrative Office of the United States Court, overseeing where these taps are kept across the street, says the average wiretap is 19 days. Why 90? Why 1 year?

Senator KENNEDY. Your statement in its entirety will be printed in the record of this hearing.

[Material follows:]

PREPARED STATEMENT OF PROF. WILLIAM W. GREENHALGH, GEORGETOWN UNIVERSITY LAW CENTER

"THIS SACRED RIGHT"

Berger v. *New York*, 338 U.S. 41 (1967) is the benchmark by which the constitutionality of S. 1566, known as the Foreign Intelligence Surveillance Act of 1977, must be measured. Mr. Justice Clark stated at 49 et seq.:

"The law, though jealous of individual privacy, has not kept pace with these advances in scientific knowledge. This is not to say that individual privacy has been relegated to a second-class position for it has been held since Lord Camden's day that intrusions into it are 'subversive of all the comforts of society.' *Entick* v. *Carrington*, 19 How.St.Tr. 1029, 1066 (1765). And the Founders so decided a quarter of a century later when they declared in the Fourth Amendment that the people had a right 'to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures * * *.' Indeed, that right, they wrote 'shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.' Almost a century thereafter this Court took specific and lengthy notice of *Entick* v. *Carrington*, *supra*, finding that its holding was undoubtedly familiar in the minds of those who framed the fourth amendment * * *.' *Boyd* v. *United States*, 116 U.S. 616, 626–627 (1886). And after quoting from Lord Camden's opinion at some length, Mr. Justice Bradley characterized it thus:

"'The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case * * * they apply to all invasions on the part of the government and its employes of the sanctity of a man's home and the privacies of life.' At 630.

"*Boyd* held unconstitutional an Act of the Congress authorizing a court of the United States to require a defendant in a revenue case to produce in court his private books, invoices, and papers or else the allegations of the Government were to be taken as confessed. The Court found that 'the essence of the offense * * * [was] the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment.' Ibid. The Act—the Court found—violated the Fourth Amendment in that it authorized a general search contrary to the Amendment's guarantees.

"The Amendment, however, carried no criminal sanction, and the federal statutes not affording one, the Court in 1914 formulated and pronounced the federal exclusionary rule in *Weeks* v. *United States*, 232 U.S. 383. Prohibiting the use in federal courts of any evidence seized in violation of the Amendment, the Court held:

"'The effect of the 4th Amendment is to put the courts of the United States * * * under limitations and restraints as to the exercise of such power * * * and to forever secure the people * * * against all unreasonable searches and seizures under the guise of law. The protection reaches all alike, whether accused of crime or not, and the duty of giving to it force and effect is obligatory upon all * * *. The tendency of those who execute the criminal laws of the country to obtain conviction by means of unlawful seizures * * * should find no sanction in the judgments of the courts, which are charged at all times with the support of the Constitution, and to which people of all conditions have a right to appeal for the maintenance of such fundamental rights.' At 391–392.

"* * * And the *Nardone* cases (*Nardone* v. *United States*), 302 *U.S.* 379 (1937) and 308 U.S. 338 (1939), extended the exclusionary rule to wiretap evidence offered in federal prosecutions."

And then came Title III, which Mr. Justice Powell described succinctly in *United States* v. *United States District Court*, 407 U.S. 297 (1972) (hereinafter *Keith*) at 301–302:

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

"Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S. Code Sections 2510–2520, authorizes the use of electronic surveillance for classes of crimes carefully specified in 18 U.S. Code Section 2516. Such surveillance is subject to prior court order. Section 2518 sets forth the detailed and particularized application necessary to obtain such an order as well as carefully circumscribed conditions for its use. The Act represents a comprehensive attempt by Congress to promote more effective control of crime while protecting the privacy of individual thought and expression. Much of Title III was drawn to meet the constitutional requirements for electronic surveillance enunciated by this Court in *Berger* v. *New York*, 388 U.S. 41 (1967), and *Katz* v. *United States*, 389 U.S. 347 (1967)."

And now as we examine S. 1566, which, incidentally, is an epochal endeavor upon the part of the Congress to codify judicial procedures authorizing the use of electronic surveillance in the United States to obtain foreign intelligence information, we may wish to reflect upon the words of Mr. Justice Stewart in *Coolidge* v. *New Hampshire*, 403 U.S. 443 (1971) at 454–455:

"Thus the most basic constitutional rule in this area is that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.'[1] The exceptions are 'jealously and carefully drawn.'[2] and there must be 'a showing by those who seek exemption . . . that the exigencies of the situation made that course imperative.'[3] [T]he burden is on those seeking the exemption to show the need for it.[4] In times of unrest, whether caused by crime or racial conflict or fear of internal subversion, this basic law and the values that it represents may appear unrealistic or 'extrvagant' to some. But the values were those of the authors of our fundamental constitutional concepts. In times not altogether unlike our own they won—by legal and constitutional means in England[5] and by revolution on this continent[6]—a right of personal security against arbitrary intrusions by official power.' * * *.

Assuming apprehension of external subversion, still the proceeding to intrude is a drastic one. Its abuse led to the adoption of the IVth Amendment, and this together with legislation on regulating the process, should be liberally construed in favor of the individual *Sgro* v. *United States*, 287 U.S. 206, 210 (1923).

"AND NO WARRANTS SHALL ISSUE"

Let us therefore examine the three essential elements of constitutional procedure with which there must be compliance with the Fourth Amendment before an intrusive statute can pass constitutional muster. The first is the Constitution's warrant prior approval requirement. The warrant tradiionally has represented an independent assurance that an arrest, search or intrusion will not proceed without probable cause to believe that a crime is being or has been committed and the person or the place named in the warrant is involved in the crime. The issuing authority, thus, must meet two tests. That person must be neutral and detached, and must be capable of determining whether probable cause exists for the requested arrest, search or intrusion.

The Supreme Court has long insisted that interferences of probable cause be drawn by "a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. *Johnson* v. *United States*, 333 U.S. 10, 14 (1948); *Giordenello* v. *United States*, 347 U.S. 480, 486 (1958). Other decisions by the Court which have mentioned review by an issuing authority prior to issuance of a warrant are *Whitely* v. *Warden*, 401 U.S. 560, 564 (1971); *Katz* v. *United States*, 389 U.S. 347, 356 (1967); *United States* v. *Ventresca*, 380 U.S. 102, 08 (1965); *Wong Sun* v. *United States*, 371 U.S. 471, 481–482 (1963); *Jones* v. *United States*, 362 U.S. 257, 270 (1960); *United States* v. *Lofkowitz*, 285 U.S. 452, 464 (1932). Whatever else neutrality and detachment from activties of law enforcement. *Coolidge* v. *New Hampshire*, supra at 450; cf. *Mancusi* v. *DeForte*, 392 U.S. 364, 371 (1968),

[1] *Katz* v. *United States*, 389 U.S. 347, 357.
[2] *Jones* v. *United States*, 357 U.S. 493, 499.
[3] *McDonald* v. *United States*, 335 U.S. 451, 456.
[4] *United States* v. *Jeffers*, 342 U.S. 48, 51.
[5] See *Entick* v. *Carrington*, 19 How. St. Tr. 1029, and *Wilkes* v. *Wood*, 19 How. St. Tr. 1153 (1763). See also *Leach* v. *Money*, 19 How. St. Tr. 1001 (1765).
[6] Paxton's Case, Quincy, Mass. Rep. 1761–1772, Appendix, p. 469 et seq. See also *Stanford* v. *Texas*, 379 U.S. 476, 481–482 (1965).

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4
93-179 O - 77 - 8

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

There can be no connection with any law enforcement activity or authority which would distort the independent judgment the Fourth Amendment requires. *Shadwick* v. *City of Tampa*, 407 U.S. 345, 350–351 (1972).

For these reasons, Section 2523(c) should be deleted as it applies to the Chief Justice consulting with the Attorney General and the Director of Central Intelligence. Secondly, consideration should be given as to whether the Chief Justices should be involved at all in the resignation process as proposed in Section 2523(a) and (b). I can foresee an ultimate recusal problem of the highest magnitude. This Subcommittee may therefore wish to consider Mr. Justice Powell's suggestion in *Keith*, supra at 323 that "the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court." Perhaps, the Chief Judge of the eleven United States Courts of Appeals could designate a single district court judge within their Circuit to entertain applications and grant orders as well as create a special court of review.

"BUT UPON PROBABLE CAUSE"

The next constitutional hurdle that an intrusive statute must clear is the probable cause requirement. *Berger* v. *New York*, supra at 55. Although a reviewing court will pay substantial deference to judicial determination of probable cause, the court must still insist that the issuing authority perform his "neutral and detached" function and not serve merely as a rubber stamp for the executive. *Aguilar* v. *Texas*, 378 U.S. 108, 111 (1964). In this connection, since Section 2526(c) provides for a statutory exclusionary rule (cf. *Gelbard* v. *United States*, 408 U.S. 41 (1972)), a reviewing court, thus, has duty to determine whether the showing of probable cause was sufficient to justify the intrusion authorized. But this duty to determine requires an adversary proceeding and not a screening of the application, order, and transcript of surveillance in camera by the reviewing court. *Alderman* v. *United States*, 394 U.S. 165, 80–185 (1969). The Supreme Court long ago conferred upon defendants in federal prosecutions the right, upon motion and proof, to have excluded from trial evidence which had been secured by means of unlawful search and seizures. *Weeks* v. *United States*, supra. The guiding hand of counsel must be present to prosecute a valid Fourth Amendment claim. *Simmons* v. *United States*, 390 U.S. 377, 394 (1968). The option is either disclose or dismiss.

The traditional test in deciding whether probable cause exists for the issuance of a warrant, it is necessary to determine whether the affiant has reasonable grounds, at the time of making the affidavit and the issuance of the warrant, for believing that the *offense charged* was being or had been committed (emphasis added). Although *Camara* v. *Municipal Court*, 387 U.S. 523, 539 (1967), *Keith*, supra at 322–323, and *Almedia-Sanchez* v. *United States*, 413 U.S. 266, 275–285 (1973) have recognized that a warrant might issue on other than traditional probable cause in certain circumstances, a fortiorari, the application as well as the order in S. 1566 must be very circumscriptive, precise and discriminate. *Osborn* v. *United States*, 385 U.S. 323, 329–330 (1966). The looser a standard necessitates the lighter a warrant. Consideration, therefore, should be given to requiring positive instead of probable cause. *Jones* v. *United States*, 357 U.S. 493, 498 (1957). In any event, the showing of justification must match the degree of intrusion. *Berger* v. *New York*, supra, at 69.

Regarding demonstrative need, another problem must be confronted. That is a thing called "clandestine intelligence activities." Such language, especially in the context of less than probable cause for believing that such activities either would be harmful to the security of the United States or involve or will involve, either as a principal or aider and abettor, a violation of the criminal statues of the United States, may be void for vagueness. *Papachriston* v. *City of Jacksonville*, 405 U.S. 156, 162 (1972). Secondly, a direction by Congress to the executive to tap persons knowingly engaging "in clandestine intelligence activities" may not pass Fourth Amendment constitutional muster. If "clandestine" is tantamount to "car prowling", the statute may be in serious trouble. *Papachristour*, supra at 169. As difficult as it may be, the words must be more clearly defined.

AND PARTICULARLY DESCRIBING

The last command that the warrant clause is designed to control is that of particularity. It prevents the issue of warrants on lose, vague, or doubtful bases of facts. It emphasizes the purpose to protect against all general searches. *Go-Bart Importing Co.* v. *United States*, 282 U.S. 344, 357 (1931). The requirement that warrants shall particularly describe the things to be seized makes general

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant. *Marron* v. *United States*, 275 U.S. 192, 196 (1927).

Section 2525(b)(I)(C) (and (c) are, therefore, immediately suspect. The executive is awarded a roving commission to seize any and all conversations. It is a general warrant. *Berger* v. *New York*, *supra* at 59. To permit the executive to use a seemingly precise and legal warrant only as a ticket to tap a person's telephone would then allow him to launch forth upon unconfined searches and indiscrimiate seizures as if armed with all the unbridled and illegal power of a general warrant. *Stanley* v. *Georgia*, 394 U.S. 557, 572 (1969).

Authorization of tapping for a three-month period is the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause. This blanket grant of authority to intrude is without adequate judicial supervision or protective procedures. *Osborn* v. *United States*, *supra*; *Berger* v. *New York*, *supra*, at 59. This indiscriminate sweep of the three-month period, as well as the one year duration in Section 2525(c) is constitutionally intolerable. It is false to the terms of the Fourth Amendment, false to its meaning, and false to its history. *Stanford* v. *Texas*, supra, at 486. Both Rule 41(c) of the Federal Rules of Criminal Procedure and the *Sgro* case, supra, call for 10-day seizures. Why should not the Congress make it unanimous.

Senator KENNEDY. Mr. Watters, you may proceed.

STATEMENT OF DAVID WATTERS, ON BEHALF ON THE AMERICAN PRIVACY FOUNDATION

Mr. WATTERS. I will be very brief.

In considering electronic surveillance within the United States operating under the aegis of S. 1566, there is no question that a large number of innocent persons would lose the privacy of their communications by virtue of its provisions.

Senator KENNEDY. Of which provision?

Mr. WATTERS. S. 1566.

Senatory KENNEDY. We haven't anything on the books now. The right of privacy certainly isn't being protected at the present time.

Mr. WATTERS. That is correct.

It is estimated that over 95 percent of the interceptions done under this act will be of the communications of innocent Americans.

The current wiretap law, Title III, specifies that—

> Every wiretap order shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception * * *

Clearly, this stipulation means that the privacy of a person will be more greatly secure if a method is devised whereby a lesser volume of innocent private communication is acquired.

Unfortunately, most of the discussion in open hearings before the Senate Judiciary Committee and before the Senate Select Committee on Intelligence dealing with the subject of minimization has focused on the matter of expungement of irrelevant information already intercepted..

In the dialog relating to expungement as a means of minimization, it is presumed that if expungement is required through the execution of a set of relevance tests respectively applied to each communication or part thereof, then expungement, meaning destruction of the materials involved, will, in fact, occur. The paradox which arises in this presumption is derived from the cardinal principle in intelligence work, domestic or foreign, that little be thrown away.

Certainly an expungement clause should be included in a National Security Communications Surveillance Act. It is not believed, how-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

ever, that as a practical matter it will do much in minimizing information retained once it is obtained.

The provisions of the S. 1566 minimization procedures, other than the mere mention of the need for acquisition limitation, are primarily directed toward expungement of information and methods of information retrieval.

Senator KENNEDY. This is part of the problem. The ACLU says that they do not want it expunged. You want it expunged.

Mr. WATTERS. In reality, acquisition minimization at the front end is easier to control and more effective than is the expungement kind. It is less subjective in nature and more difficult to circumvent.

We are prepared to recommend a series of acquisition minimization criteria which would be appropriate in wiretap law in general. Such criteria, I believe, would be appropriate for conventional criminal surveillance as well as espionage criminal activity which S. 1566 should be addressing.

Mr. Chairman, I will not burden you with the technical details of the following minimization criteria. In brief summary they say this: First, that the tape recordings of lawful wire tap or electronic bugging operations must be examined at least once in every 24-hour period to determine if the objectives of the court order have been met.

Second, that stricter standards of cause and closer judical supervision shall be applied when operations are expended beyond the first acquisition of the target information.

Third, that random and systematic plungering through our multicircuit microwave and satellite long-lines systems will cease altogether, there being alternative, less intrusive means of getting the desired target information.

The balance of my written testimony concerns this and other aspects of minimization. They are: (1) levels of minimization; (2) sophisticated wiretap practice; (3) probable cause; (4) limitation of warrant to 30 days; and (5) grace periods, namely the 90-day warrantless test period and 24-hour warrantless emergency provisions.

Unless you prefer that I do, I will not go into these at this time. If we had enough time, it might be appropriate to go into a real problem area, namely, broad band interception.

In any event, I ask that the remainder of my text be made part of the record.

Perhaps at this time you may have some questions.

Senator KENNEDY. We will include your statement in the record and then we will have a chance to examine them.

[Material follows:]

PREPARED STATEMENT OF DAVID L. WATTERS [1]

MINIMIZATION CRITERIA

Mr. Chairman, it is appropriate that the subject of minimization be addressed.

In considering electronic surveillance within the United States operating under the aegis of S.1566, there is no question that a large number of innocent Ameri-

[1] David Watters is a telecommunications engineer and aerospace scientist. He is a consultant on policy matters relating to electronic surveillance and security. He is the Washington representative for the American Privacy Foundation. In earlier years he was with the communications research and development branch of the Central Intelligence Agency. Earlier yet, Mr. Watters was with the Western Electric engineering arm of A.T.&T. He is a native of Georgia.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

cans would loose the privacy of their communications by virtue of its provisions. Even those persons who may be suspected of nefarious activity against the security of this country but who are later found uninvolved would have the most personal matters of their private lives exposed—matters which have nothing to do with information targeted for interception. In effect, the homes and businesses of numerous persons would be entered secretly, their property removed, and they would never know that their most intimate and personal expressions had been compromised. It is estimated that over ninety-five (95) percent of the interceptions under this act will be of the communications of innocent Americans.

The Supreme Court has ruled that electronic surveillance such as wiretapping and bugging is a search and seizure falling under the terms of the Fourth Amendment to the Constitution. The Court also has ruled that in all cases a warrant must be obtained before wiretapping may proceed—no executive privilege.

It has been argued, and rightly so, that a wiretap is, by nature, an unreasonable search and seizure and therefore unconstitutional. The majority of information obtained through a wiretap, in most cases, will have nothing to do with the targeted information sought under a court warranted order. Additionally, there will be great likelihood that privileged information will be compromised in any one such operation; e.g., lawyer-client, doctor-patient, priest-penitent, or husband-wife.

Set aside, however, the foregoing argument for the moment and consider briefly the premise that it is actually possible to conduct a wiretap operation in a way which will cause it to approach the criteria of the fourth amendment, that "the rights of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." It will then be necessary to establish some practical rules and guidelines for the persons who shall conduct lawful wiretaps which will constrain each such operation to more nearly become and resemble the kind of specific search for specific items held by specific persons as described in the constitution. These rules and guidelines, then, are the minimization procedures we are addressing.

As we review S.1566, the so-called Foreign Intelligence Surveillance Act, we should look at its definition of Minimization Procedures which are given on page 8 starting at line 1. This is the eighth definition under Section 2521 dealing with definitions.

Here we have one long sentence which rambles on for over a page and a half attempting to establish some reasonably designed minimization criteria. The statement is logically convoluted, syntactically awkward, vague in reference, and means very little in terms of real restriction to the scope of any individual wiretap operation.

The current Title III wiretap law specifiies that "Every (wiretap) order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in a such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days."

These requirements find their roots in Title III, Chapter 119, Section 2518, paragraphs (1) (d), (4) (e) and (5).

Clearly, this stipulation means that the privacy of a person or the public in general will be more greatly secure if a method is devised whereby a lesser volume of innocent private communication is acquired.

Unfortunately, most of the discussion in open hearings before the Senate Judiciary Committee and before the Senate Select Committee on Intelligence dealing with the subject of minimization has focused on the matter of the expungement of irrelevant information already intercepted, recorded and analyzed. This is a poor substitute for minimization procedures referred to in Title III, the wiretap law.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

In the dialogue relating to expungement as a means of minimization, it is presumed that if expungement is required through the execution of a set of relevance tests respectively applied to each communication or part thereof, then expungement, meaning destruction of the materials involved, will, in fact, occur. The paradox which arises in this presumption is derived from the cardinal principle in intelligence work, domestic or foreign, that very little be thrown away. They cannot bear to throw out the little nuggets gleaned surreptitiously even though each has no bearing on the direct subject of suspicion. "Who knows," it is reasoned, "when we shall find it helpful to use a bit of information which today seems innocuous, but which later when pieced together with other innocuous information may form a pattern which becomes meaningful." All information, no matter how trivial, may be used to construct a behavior pattern or character analysis. Any personally sensitive tidibits of information, though they relate neither to national security nor foreign intelligence, may be useful to intimidate a person, entrap a person, or discredit a person. These tidbits, therefore, are not likely to be thrown away. We have seen through decades of snooping by the FBI that this agency cannot bear to bring itself to destroy irrelevant raw data files even when the information is proven to be complete fabrication.

Certainly an expungement clause should be included in a National Security Communications Surveillance Act such as we are considering here. It is not believed, however, that as a practical matter it will do much in minimizing information retained once it is obtained.

The provisions of the S. 1566 minimization procedures, other than the mere mention of the need for acquisition limitation, are primarily directed toward expungement of information and methods of information retrieval. Incidentally, this bill would prohibit retrieval of private information by the name of a "United States person", but would permit retrieval by any other identification criterion. This apparent protection disappears when one considers the many other ways such information may be retrieved by cross correlation of categories. By example, the computer system might be interrogated, "give me the names of all democratic senators from Massachusetts who traveled in Europe in the years between 1965 and 1975."

Perhaps much of the discussion in congressional hearings has centered around the expungement kind of minimization rather than acquisition minimization because expungement is more easily understood than is the surveillance technology of acquisition and the nuances of implementing an electronic interception.

In reality, acquisition minimization at the front end is easier to control and is more effective than is the expungement kind. It is less subjective in nature, and more difficult to circumvent.

The courts have generally agreed that a procedural method for the minimizing of the acquisition of information in a wiretap operation is necessary, though they are seldom in agreement as to just what method shall be applied.

It must be understood that the intelligence community resists most vigorously any attempts to restrict their activity by front-end acquisition minimization. Such restriction slows down their operation, is more cumbersome to instrument, and is less efficient. Further, it requires more accountability to the courts in particular and to the records in general. It does not mean, however, that the intelligence community is, in reality, deprived of any real surveillance objective sought after. It simply means that an equitable tradeoff between wholesale instrusion and privacy is achieved.

One hesitates to discuss degrees of efficiency in the use of electronic surveillance. There are no substantive figures to support the cost-benefit justification of the total body of national security interception into communications common carrier, telephone and telegraph transmission now being undertaken within the United States. It is questionable that the whole operation could survive a rigorous zero-based budgeting purge.

There is no doubt that the intelligence community is vigorously resisting the imposition of effective acquisition minimization rules set forth by Congress. I believe that the intelligence and investigative agencies fear definitive front-end minimization requirements more greatly than unfavorable shades in the definitions of probable cause, or of national security, of foreign agent, or of hostile foreign power. Unless explicit minimization criteria are set forth in the wiretap laws themselves, not left to inference or to the discretion of the wiretapping agent or to notes in the minutes of hearings, then the principle of minimization will be largely ineffectual.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

We are prepared to recommend a series of acquisition minimization criteria which would be appropriate in wiretap law in general. Such criteria, I believe, would be appropriate for conventional criminal surveillance as well as espionage criminal activity which S. 1566 should be addressing.

The minimization criteria which are presented here are an expansion of the *James* Criteria developed by Judge Robinson in a landmark case in the District of Columbia in 1974 and largely take the form as presented in the Michigan Senate Bill No. 1536 last year, and in H.R. 7139 introduced here last month by Representative Kildee.

ACQUISITION MINIMIZATION CRITERIA FOR THE "FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1977"

No order entered under this section may authorize or approve the interception of any wire or oral communication for any period longer than is necessary to achieve the objectives of the authorization, nor in any event longer than thirty days. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection ( ) of this section and the court making findings required by subsection ( ) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for more than thirty days. Every order and extension thereof shall contain a provision that the interception shall be executed as soon as practicable, shall be conducted in such a way as Every order and extension thereof shall contain a provision that the interception tion under this act, and must terminate upon attainment of the authorized objective, or in any event in thirty days.

(*a*) In minimizing interception of all or parts of communications not otherwise subject to interception the applicant for a court order shall use means, whenever practicable, which employ on-line monitoring of wire or oral communications by the authorized agent, himself, at the time of and during the intercept operation. When monitoring of communication at the time of interception is not practicable, the fruits of such interception, wire, tape or other recordings, registrations, records, information or data must be examined concurrently at least once in each twenty-four hour period by the authorized agent to determine if communication described in the court order in fact has been intercepted. In either case the interception activity shall cease and terminate when the described communication has been first obtained. Neither monitoring nor interception shall take place during periods of time when there is no reasonable expectation of interception of communication described in the order.

(*b*) When the scope and complexity of the hostile activity under investigation indicates that interception beyond the first incident of communication acquired as named in the court order is necessary; the authorizing judge may give authority for expanded interception: *Provided that:*

(i) at the time of application the applicants seeking the order shall certify to the judge that expanded operations will be necessary to intercept communications of a large scope of persons engaged in the hostile activity of a foreign power; and

(ii) when the subject telephone, telegraph instrument, communication equipment or circuit to be intercepted is known in evidence by the applicant at the time of the application to be used largely in the hostile activity of a foreign power; and

(iii) there is an agreement and adherence to continuous judicial supervision of the interceptiton operations and periodic judicial examination of the fruits of such interception during the tenure of such interception; and

(iv) there is an agreement and adherence to the principle that, if, in the process of the expanded interception, the intercepting agent or the court find that the contents of the intercepted communications reveal that the hostile activity of a foreign power under investigation is of a lesser degree than was originally anticipated, the expanded interception will be terminated; and

(v) there is examination of the fruits of the interception concurrently at least once every twenty-four hour period by the person authorizing the application or his agent; and

(vi) efforts are made to eliminate monitoring and interception of communications during periods of time when there is no reasonable expectation of interception of communication described in order.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

(*c*) In order to prevent the interception of all or parts of wire communications not otherwise subject to interception, the applicant for a court order and his agent shall neither in any case of expanded operation nor otherwise use broadband interception techniques wherein simultaneous circuits not being employed by persons engaged in the hostile activity of a foreign power are intercepted. Random or systematic scanning among wire communications circuits or channels in order to discover, identify, acquire or otherwise intercept the communications of persons for national security purposes is strictly prohibited under this act.

(*d*) In minimizing interception of all or parts of wire communications not otherwise subject to interception, the applicant for a court order shall use means, whenever practicable, to access the wire communications circuit specified for interception at a point in the communications network wherein the authorized agent and his interception equipment, electronic, mechanical, or other devices have and will have exposure and general access to the least number of other circuits not specified for interception.

Levels of minimization

The acquisition minimization criteria as proposed set forth two major levels of intrusion:

The first takes on the character of an individual criminal investigation, and is generally more protective of privacy and civil liberty. It is expected that this set of minimization requirements will be used when an operation is directed against or toward one or a few number of persons. There are the criteria to be employed in the great majority of national security wiretapping cases. This first case requires that the tap be removed after the first acquisition of communication containing information relating to activity damaging to national security.

The second level takes on the character of an expanded criminal intelligence operation. This would be directed toward a broader conspiracy of persons engaged in hostile activity. The main difference is that in this latter case, the interception under the court order may continue beyond the acquisition of the first communication containing information relating to activity potentially damaging to the security of our nation. Also in this latter case, more stringent justification of cause must be supplied the court in order to initiate this less frequent kind of surveillance operation.

Normally the first level of minimization requirements would be imposed as the first if not the only level in an intelligence operation. If the findings of the evidence before the court as obtained by the initial first level probe so justify, the judge may expand the operation into level two.

It is to be noted that in both cases, level one and level two, that the wiretapping agent must examine the fruits of the intercept at least once each day to determine if the operation is productive. He also must turn off his interception equipment so as not to collect or otherwise record communications occurring during periods of the day when there is no expectancy or little probability that activity inimical to national security shall occur on the circuit. As a general rule, neither of these criteria are being applied in criminal or national security taps at present.

Wiretap practice

The public at large has the image that a wiretapper is a little man with earphones and a tape recorder hidden away in some closet. For the most part, however, government wiretapping does not employ this method. If it were so, it would be much more reasonable to expect the little man to disconnect the recorder during irrelevant messages and to remove the interception system after the first "damaging" communication has been captured. Thus the interception of communications not specified in the court order would be greatly minimized.

The present, most simple, practice of the government in wiretapping today, however, is to place an automatic tape recorder across the line of a suspected criminal or intelligence target and leave it in place for at least a whole month. Examination of the tapes may take place once or twice toward the end of the month. More likely than not, the examination of the tapes begins only after the month is completed. The tape recorder is seldom hidden away in a closet, but rather is among a bank of such recorders installed in a locked office across town or across the state. Being automatic, the recorder turns on only when the telephone or telegraph circuit is active. The recorder is generally left unat-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

tended except for a few moments for an agent to remove and renew tapes every few days or weeks. Thus, little attempt to minimize is made. The requirement that human examination of the tapes be done every twenty-four hours should make a dramatic impact on minimization. Such a requirement, naturally, would be looked upon unfavorably by investigative and intelligence agents. Our objective, however, is not to make things as easy on the agent as technology would allow, but rather to more greatly maximize privacy and minimize intrusion into the personal lives of individuals. The twenty-four hour examination rule is considered to be a reasonable compromise between continuous, on-line, agent monitoring and infrequent tape examination such as only once or twice a month.

The elimination of recording during certain periods of the day when there is no expectation of capturing a target communication should cause no appreciable hardship. Timing devices already on many automatic recorders would be so employed. Presently, little use is being made of such devices.

Cause

In using electronic surveillance by secret intrusion into communications over a common carrier circuit, there is great danger in abuse and in setting a precedent for change in the traditional criminal standards of probable cause.

We are reminded that although the Constitution of the United States sets forth basic rights of U.S. citizens as "we the people", it, in a certain sense, declares basic principles of human rights for all people; even those who may be suspected as being agents of a foreign country.

The criteria of probable cause, then, should be the *minimum* recommended standards for initiating a wiretap order for both conventional criminal and national security espionage cases. Thus, probable cause would be required as a minimum justification for establishment of an electronic surveillance by interception of a telephone or telegraphic communication using the first level of minimization requirements. This level, as mentioned in the paragraphs above, would be the most protective of privacy of the two levels recommended.

In order to initiate wiretap operations under level two minimize conditions, an even greater level of certitude of nefarious activity should be provided the court. Since level two minimization would permit an interception operation to be expanded beyond the acquisition of the first target communication, such an operation would become more intrusive and tend to diminish privacy to a greater degree than would level one. Hence, it is our opinion that a confidence test of evidence for the establishment of a level two operation must be greater and more stringent than mere probable cause.

Confidence levels of certitude that a crime or hostility has been, is being or is likely to occur might be placed on a scale of one to ten, thus:

(1) No Possibility.
(2) Scintilla of Possibility.
(3) Reasonable Suspicion.
(4) Reasonable Likelihood.
(5) Substantial Basis.
(6) Probable Cause.
(7) Preponderance of Credible Evidence.
(8) Clear and Convincing Proof.
(9) Beyond a Reasonable Doubt.
(10) To a Certainty.

It may be seen on this scale, then, that probable cause falls just below the median. This is the recommended test for level one minimization interception.

In the case of level two minimization criteria application to a wiretap operation, it is recommended that the next more rigorous test of the certitude scale be applied, namely, "the preponderance of credible evidence."

Hence, in the language of the proposed level two minimization criteria for the Foreign Intelligence Surveillance Act, there are phrases which will act as a guide to the court to indicate what shall constitute a preponderance of credible evidence; (a) a large scope of persons must be involved in the hostile activity of the foreign power, and (b) the communications circuit to be intercepted must be used largely in this activity.

Thirty days

It is to be noted that a court order for wiretapping or any order of extension in the minimization criteria proposed here would be limited to a thirty-day operation. A thirty-day limitation is imposed in the current Title III wiretap law. The

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

statutory length of a wiretap operation, certainly, is a criterion of "minimization of interception." It is our opinion that the ninety day wiretap order as is specified in the bill before us, S. 1566, is unnecessarily intrusive and ought not to be suffered. We are reminded that it was recommended by members of the Federal Wiretap Commission that national security wiretap orders be limited to fifteen days. We should be willing to compromise and hold the line at the currently legal thirty-day tenure.

Broadband interception

Perhaps the most abusive of all of the wiretap practices now being undertaken by the federal government in America is broadband, random and systematic prowling throughout our telecommunications systems by the National Security Agency and others. This broadband, vacuum cleaner, practice is widespread throughout the country. It is pervasive and potentially highly destructive of the privacy, freedom and liberty we cherish.

By broadband interception we mean that kind of wiretapping wherein the government places electronic surveillance on a large number of parallel communications circuits simultaneously. This practice may be done by interception of major trunk lines within or between cities. Such practice is being done with or without the complicity of the telephone company. It is being done by interception of major cross-country microwave link pinch points each containing tens of thousands of message circuits. This is in addition to similar surveillance on the primary U.S. electronic portals for foreign telecommunications traffic.

Broadband interception by the federal government has been growing steadily since World War II. It gained its initial thrust by a secret executive order by President Franklin Roosevelt under recommendation of Secretary of Defense Forrestal. It began its climb with the institution of the National Security Agency. In review of the orders and documents on this subject, one is hard pressed to find that Messrs. Roosevelt and Forrestal intended that broadband interception, as such, should occur at all. Rather, one is driven to the conclusion that this particular interpretation has been the invention of the military establishment.

One reason that broadband interception has continued to be applied without check for so many years is that it is so complex technically that those few in the White House and on Capitol Hill who have known about it have been unable to understand what it really means.

It was just this sort of threat that Supreme Court Justice Brandeis had in mind as he spoke of government intrusion when in his famous dissent in *Olmstead* v. *United States* he said ". . . writs of assistance and general warrants are but puny instruments of tyranny compared to wiretapping."

Today the federal government is stalking at random throughout our telecommunications common carrier circuits. In most cases, this is being done without a court order. In the greater majority of these intercepts, there is no specific order from the Attorney General. Rather, this activity is being done on a blanket order similar to the general warrant or writ of assistance—the very kind of behavior instituted by the King of England more than two hundred years ago. This was a major irritant over which the American Colonies fought the Revolutionary War.

It is no wonder that the National Security Agency terminated "Operation Shamrock" as soon as the House Government Operations Committee and the Senate Select Committee on Intelligence began to expose this horrible practice to the public. Operation Shamrock, it will be recalled, was that practice wherein several government agencies had secured physical hard copies of virtually every telegraphic cable sent to and from the United States for the past thirty years. This was done by midnight visits to the various cable companies within the United States.

It is no wonder that the National Security Agency gave up Operation Shamrock with not even a whimper of objection. Operation Shamrock had long been obsolete and redundant to the modern technological advances of broadband interception.

The fact of the existence of broadband interception throughout the land is perhaps the most jealously kept secret in America. Witness the curious fact that the executive branch has refused on executive privilege to furnish the Congress, on subpoenae, only two groups of evidence. One was the White House Watergate tapes. The other was the AT&T correspondence with the Department of Defense

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

regarding interception assistance given by the telephone company. It is reckoned by the Moss Subcommittee that the reluctance to disclosure of this latter group has not been so much out of fear of revealing targets of surveillance as letting the cat out of the bag regarding broadband interception of telephonic and telegraphic communications.

Let there be no misunderstanding, it is not the Soviets who are being kept in the dark about broadband operation—they know quite well what is going on. It is the American people who are unaware of its existence.

On reflection, it may be seen that broadband interception is potentially much more damaging than the writ of assistance or general warrant. First, one must observe that a broadband intercept surveillance operation injected into a single microwave link, for instance, permits the scanning of hundreds of thousands of messages in a single day with sophisticated computer-like equipment operated unattended, or by one or two persons. Contrast this with the thousands of agents of the Crown who would have been required to search through the private papers of the homes of everyone in Baltimore.

Secondly, one must observe that a broadband intercept surveillance operation is done completely in secret—no one knows when he has been scanned. Contrast this with the fact that in colonial times the citizen whose home had been ransacked by an agent of the king was aware of the search and seizure because he usually was there and saw the operation take place.

Broadband interception has such a great pervasiveness and potential for abuse that it is recommended that this practice be abolished altogether by the language of the proposed minimization criteria. Paragraphs (*c*) and (*d*) of the proposed minimization criterial carry this prohibition. The words of paragraph (*c*) would strictly forbid this practice. The composition of paragraph (*d*) is implicit to show that the same wire communications sought after in wideband interception may, in fact, be acquired by other, less intrusive, technological methods. Here, in effect, the stipulation is made that the interception must be made on the direct current, single subscriber, line rather than on inter-city trunk lines. Implicit in this latter paragraph, also, is the theme that government wiretapping agents shall stay out of telephone exchanges, communications conduits, and junction boxes. Rather, these agents acting on court order may be provided "drawn loops" on specified lines to a listening post, a service often provided by the telephone company.

Lest there be some misunderstanding about broadband interception, it must be borne in mind that a recording is not necessarily made of every communication message transmitted over all circuits of a trunk line. Rather, an on-line scanning is made of each and every message to determine if certain tell-tale elements are present. This real-time or near real-time scanning is achieved at lightening speed and is completely automatic.

It must be understood that when a warrant would be issued for a certain targeted objective to be sought through the broadband system, this does not ordinarily mean that special equipment is installed for that objective alone. The equipment is already in place in our microwave long lines network. What it really means is that a new set of punched cards are inserted into the system to operate as a new addition to the watch list of called telephone and telegraph numbers or to the trigger word lexicon.

In the case of voice transmissions, the criterion which causes a conversation to be placed in permanently recorded form, or in the intelligence parlance to be "dropped out", is the address code which precedes the transmission. The address codes correspond to the called party telephone number, and occur in the form of the multi-frequency tones one hears when a long distance call is placed.

In the case of non-oral transmissions such as Telex, the multi-frequency address codes are used as a drop-out criterion similar to the voice interception case. An additional set of drop-out criteria also are imposed in this non-oral communication case which is even more highly selective. This second criteria set is constructed from key trigger words or phases, or is syntactically formulated to recognize certain national languages.

The intelligence community has chosen to restrict the meaning of "intercept" to those voice communications which are actually dropped out for further analysis. They choose not to consider the acquisition of non-oral communications, Telex, and the like, as an intercept under the definitions of Title III.

The multi-frequency tones codes associated with all toll telephone calls and Telex transmissions are similar or analogous to the address on the outside of a

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

letter. It was recently found that the Postal Service for years has been exercising surveillance on many citizens and residents within the United States without court orders by copying down the address and return address on the outside of envelopes. These mail covers were conducted to an order of magnitude of about one-hundred to one times as many actual mail opening by the Post Office and other agencies. Such mail cover activity without court orders has of late been terminated by direction of Congress.

Wire covers, however, continue to abound without court orders. They range into an order of perhaps more than one thousand times the number of actual acquisitions of the "body" of telecommunication messages. This switch-and-signal type of interception involving multi-frequency tones, pen registers, and other computer-like systems must be made to come under the control of our wiretap laws and must be restricted to court ordered application. The proposed minimization criteria are phrased in such a way as to prevent these unwarranted abuses. This coupled with a redefinition of the term "intercept" should bring the practice under control.

Grace periods

A curious stipulation of S. 1566, the Foreign Intelligence Surveillance Act, would allow a ninety-day grace period without a court order for the installation and testing of interception equipment. This provision is coupled with the requirement that any interceptions made during the ninety-day test period will be destroyed.

We strongly disagree with allowing a "free" warrantless interception test period. This grace period will simply become another inroad for governmental abuse. The test period proviso will become an umbrella to protect unlawful interception should the operation be discovered.

It must be noted that the real reason, other than the obvious as given above, for the ninety-day test period is to allow the installing, tuning, programming and debugging of the broadband microwave land line and satellite interception systems currently being installed across the country by the National Security Agency. Lesser sophisticated systems do not require the degree of special adjustment, tuning and programming necessary for a broadband microwave tap. The more simple interception equipment may be tested on dummy communications networks rather than on national communications common carrier circuits while actually transmitting private messages.

The ninety-day test grace period argument, it may be seen, becomes largely moot when broadband interception would become unlawful.

Again, one is reminded that by giving up the practice of broadband interception, the nation is not really relinquishing access to any target of a crime, national defense or intelligence. It simply means that the interception must take place in the network at a lesser level of multiplexing, or in simpler terms, at a point where fewer communications of persons not cited in the court order are exposed to interception.

The twenty-four hour emergency grace period specified in S. 1566 also becomes an avenue for abuse. This twenty-four hours is that period during which a wiretap might be installed without a court order. This practice would be allowed with the understanding that the intercepting agency will apply for the court order within twenty-four hours of the inception of the wiretap.

Again, it is our opinion that the twenty-four hour emergency grace period is unnecessary, especially in national security cases. Intelligence operations are generally of an exploratory nature. Such exploration does not require the immediate reaction that might be more justifiable in conventional criminal cases wherein an impending murder, a kidnapping or illegal drug transaction is involved.

The twenty-four hour emergency grace period, in effect, becomes a tool of coercion used to press a judge into finally signing a court order. For a judge to refuse to sign a court order involving an interception operation which has already begun will place the judge and the applicant into a working relationship of considerable embarrassment. It may be seen, then, that there will be a greater likelihood for a judge to refuse an operation which has not yet begun than to stop an operation which is already underway.

The twenty-four hour grace period becomes a fall-back position for a government wiretapper who is caught in the act without a court order. He can always say, "I was planning to go down to the court house first thing in the morning."

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Both the ninety-day and twenty-four hour grace periods imply the siege philosophy prevalent in certain halls of government. The grace periods, at their hearts, both imply certain executive privilege beyond the meaning of the U.S. Constitution. Elimination of the grace periods will be a measurable improvement in the minimization of the interception of communications of citizens not involved in criminal or hostile activity.

For those wishing to review some significant court rulings relating to minimization, the citations following will be useful.

U.S. v. *James*, 161 at 100–102, C.A. D.C. 1974, 494 F.2d 1007 at 1019–1021.
U.S. v. *Scott*, D.C. D.C. 1971, 331 F. Supp. 233.
U.S. v. *King*, D.C. Cal. 1971, 335 F. Supp. 523.
U.S. v. *Herrmann*, D.C. Wisc. 1974, 371 F. Supp. 343.
U.S. v. *Sisca*, D.C. N.Y. 1973, 361 F. Supp. 735.
U.S. v. *Lanza*, D.C. Fla. 1972 349 F. Supp. 929.
State v. *Lee*, Md. App. 1972, 295 A.2d 812.
Johnson v. *State*, 1970, 177 S.E. 2d 699, 226 Ga. 805.
U.S. v. *Leta*, D.C. Pa. 1971. 332 F. Supp. 1357.
U.S. v. *Bynum*, C.A. N.Y. 1973, 485 F.2d 490.
U.S. v. *Poeta*, C.A. N.Y. 1972, 455 F.2d 117.
U.S. v. *Falcone*, D.C. N.J. 1873, 364 F. Supp. 877.
U.S. v. *Cox*, C.A. Mo. 1972, 462 F.2d 1293.
State v. *Siegel*, Md. 1972, 292 A.2d 86.
People v. *Solomon*, 1973. 346 N.Y. S.2d 938, 76 Misc. 2d 926.
U.S. v. *Bobo*, C.A. S.C. 1973, 477 F.2d 974.
U.S. v. *Lamonge*, C.A. Ohio 1972, 458 F.2d 197.
U.S. v. *Askins*, D.C. Md. 1972, 351 F. Supp. 408.
Granese v. *State*, Ga. 1974, 206 S.E.2d 26.
U.S. v. *Kohne*, D.C. Pa. 1973, 358 F. Supp. 1053.
U.S. v. *Manfredi*, C.A. N.Y. 1973, 488 F.2d 588.
Spease v. *State*, Md. App. 1974, 319 A.2d 560.

Senator KENNEDY. Ms. Herst, in your testimony you mention that NCARL is deeply concerned about the notification provision of S. 1566. In what respect are you concerned?

Ms. HERST. I think what the gentleman said about the *Alderman* case certainly applies in that we believe people, when information gathered from an electronic surveillance is going to be used against them in a criminal case, should have an ability to get the entire logs to challenge them for taint. Simply suppression of evidence is not enough.

We are also concerned that given the ex parte in camara nature of the hearing to determine the illegality of surveillance, there is not enough opportunity for people who are overheard when that information is going to be used against them in a criminal proceeding to challenge that.

Senator KENNEDY. Your reference, then, in terms of notification is to the trial procedure; is that correct?

Ms. HERST. Yes.

Mr. GREENHALGH. I believe this was some oversight by the Department, but there is no definition of the words "aggrieved person" like there is in title III. I suggest that you add 2521(11) to make that synonymous.

Senator KENNEDY. Staff tells me that the definition in title III applies.

Mr. GREENHALGH. It does apply?

Senator KENNEDY. Professor, if you would review the legislation with regard to those different types of problems, we would welcome that.

Mr. GREENHALGH. I thought I had.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Senator KENNEDY. You pointed out the principal objections. Many of those matters we have; others we do not.

Mr. GREENHALGH. I am sorry Senator Hatch is not here because he became a little bit concerned about intervenors on a motion to suppress and rummaging through Government files as the foreign authority surveillance—it does not happen that way.

In considering this legislation you have another constitutional clause of the sixth amendment to which you have to pay very careful attention. That is the guiding hand of counsel under 3504 when he makes that motion as well 12(b)(3) under the Federal rules on a motion to suppress. He is entitled in an adversary proceeding to litigate that issue.

Senator KENNEDY. We will draw that to Senator Hatch's attention.

We will keep the record open for 15 days for any other additional comments, suggestions, or observations.

The subcommittee stands in recess.

[Whereupon, at 12:20 p.m., the subcommittee recessed to reconvene at the call of the Chair.]

GEORGETOWN UNIVERSITY LAW CENTER,
Washington, D.C., July 1, 1977.

Senator EDWARD M. KENNEDY,
Russell Senate Office Building, Washington, D.C.

DEAR SENATOR KENNEDY: Pursuant to your request of June 14, 1977, I have enlarged the review to include title III, S. 1437 and S. 1566 as they relate to eavesdropping and wiretapping in order to highlight the legal consequences of technical, or other, differences in their language. Enclosed you will find a rough chart comparing salient aspects of the three documents, noting perceived differences and inconsistencies between them.

I believe it would be appropriate for me to indicate some of my observations in this letter:

1. Use of the definitional term "court of competent jurisdiction" [S. 1437, § 3108(d)] in S. 1437 rather than "judge of competent jurisdiction" [title III, § 2510(9)] may be ambiguous in effect. Would a wiretap application be made to the entire court or to a single judge? (For example, the Federal Court of Appeals hear appeals before a panel of three judges. Would three appellate judges have to rule on wiretap applications?) Furthermore, you should note that S. 1566 amends title III, § 2511(1) to contain the phrase "court of competent jurisdiction." As I have just indicated, Title III uses "judge of competent jurisdiction" and consistency would require such language in a title III amendment.

2. Under title III, § 2510(6) "person" is broadly defined and would, for example, include corporations. Under S. 1437, "person" would have the meaning provided by § 111 which limits it to individuals. Can wiretaps be authorized against corporations? The restricted definition of "aggrieved person" [S. 1437, § 3108(a)] is one ramification of the limited definition of "person". Must pre-trial notice be given to corporations? [*see*, S. 1437, § 3106(c)]

3. Although broadly written, it is unclear whether S. 1437, § 3106(d) "official proceeding before a government agency" includes court and grand jury proceedings. Is a court a "subdivision" of the judicial branch? (Review S. 1437, § 111 definitions of "government agency" and "official proceeding.")

4. S. 1437, § 1512 seems to require a higher standard of knowledge than the similar offense provided for under title III, § 2511(a).

5. Sections 3108 (e) and (g) of S. 1437 erroneously cross-reference to 1525 (c) and (f), respectively, rather than to 1526 (c) and (f).

6. S. 1437, § 3103(c), paralleling title III, § 2518(5), respecting judicially ordered time limitations deletes language that an extension be no longer than "the judge deems necessary." It appears this deletion would remove a Government argument that a longer than necessary extension fell within a judge's realm of discretion in any appeal based upon the length of an extension that was too long.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

7. S. 1437, § 3106(a)(1) would delete the limitation of title III, § 2517(1) which allows disclosure of interested information only to other law offices without a court order. Under S. 1437 the only standard would be "proper performance of his official duties."

8. S. 1437 expands the category of law officers who can request authorization to apply for wiretapping orders. (Compare S. 1437, § 111 "law enforcement officer" to title III, § 2510(7) "investigative or law enforcement officer.")

9. S. 1437, § 3105(b) enables a motion for "evidence derived from such contents." [re: emergency interceptions]. Such language is not contained in the parallel title III, § 2518(8)(d).

10. Although not explicitly stated, title III, § 2513, respecting confiscation of devices, would apply to ch. 120 electronic surveillance violations in those instances S. 1566 amends title III, § 2511 to include ch. 120 electronic surveillance. [§ 2511(1) (a), (c), (d)]. Furthermore, title III, § 2512 violations probably silently include ch. 120 electronic surveillance situations and therefore also allow confiscation.

11. It is unclear whether S. 1566, § 2524(c), giving judicial officers the authority to request additional "information", is broader or narrower than the title III, § 2518(2) authority to request additional testimony or documentary evidence.

12. S. 1566 does not appear to authorize judges to require periodic reports pertaining to the progress of ch. 120 electronic surveillance analogous to title III, § 2518(6) powers regarding ch. 119 interceptions. However, should an extension be requested, a judge would have the power to gain the substance of such information under § 2525(c).

I hope the prepared chart proves useful. However, I must caution that it is difficult to compare these documents. Although it is relatively easy to see the changes made by the S. 1566 conforming amendments to ch. 119 (title III) as they generally serve the purpose of including some portions of ch. 120 under ch. 119 provisions and excluding others, a comparison of the relative procedures between ch. 119 interceptions and ch. 120 electronic surveillance is problematic because each proceeds from a different base. Similarly, S. 1437 although generally paralleling title III, is almost impossible to compare in the crucial areas. For example, a proper comparison of the enumerated offenses for which a wiretap application may be made would virtually require a complete review of all of the title 18 crimes listed in § 2516(1) and their analogs under S. 1437.

I am glad to have been of service to this Subcommittee in these matters. If you have any further questions, please do not hesitate to call.

Most sincerely,

WILLIAM W. GREENHALGH.

Title III	S. 1437	S. 1566
Sec. 2518(10)(b) appeal	Sec. 3724(b), (c) enables Government appeal from suppression grant or application denial, no stated appeal period except for "due diligence" (FRAP, however, requires appeals within 30 days).	Title III, sec. 2518(10)(b) unamended; unclear whether ch. 120 suppression grant appealable through normal processes or through special sec. 2523(b) court (see language of sec. 2526(c), last sentence (under present wording probably normal processes).
Sec. 2519 reports	Sec. 3107 virtually identical to title III; in addition it gives administrative office rulemaking authority to require the court, and attorney general or State prosecutors to report according to any additional form or content rules; also adds requirement that prosecutive reports include "summonses" as well as arrests.	Title III, sec. 2519(3) amended to limit reports to Congress to ch. 119; sec. 2527 added to require the attorney general to report to administrative office and Congress only total number of applications and their disposition (granted, denied, etc.) for ch. 120.
Sec. 2520 civil recovery	Only corollary is sec. 4103 providing civil action against eavesdropping offender which is substantially the same as title III, sec. 2520 in effect with respect to S. 1437, sec. 1521 violations.	Title III, sec. 2520 amended to give civil action against violative wiretapping under both ch. 119 and 120 except to foreign powers or their agents if neither U.S. citizens or aliens permanently residing in United States.
Definitions:		
Sec. 2510(1) wire communication.	Not defined	Adopts title III, sec. 2510(1) definitions; see sec. 2521(a).
Sec. 2510(2) oral communication.	Sec. 1526(f) private oral communication; rephrased but substantially the same as title III, sec. 2510(2). [Note, erroneous cross-reference in sec. 3108(g) to sec. 1525(f).]	Adopts title III, sec. 2510(2) definition; see sec. 2521(a).

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Title III	S. 1437	S. 1566
Sec. 2510(3) State	Sec. 111 substantially the same as title III, sec. 2510(3).	Adopts title III, sec. 2510(3) definition; see sec. 2521(a); sec. 2521(b)(1) defines foreign power and sec. 2521(b)(2) defines agent of a foreign power.
Sec. 2510(4) intercept; ". . . aural acquisition of the contents of any wire or oral communications . . .".	Sec. 3108(f) substantially similar; deletes "aural" in defining type of acquisition, explicitly includes recordation. (Does deletion of aural affect status of pen registers?)	Adopts title III, sec. 2510(4) definition; in addition there is sec. 2521(b)(6) electronic surveillance definition (defined as various types of acquisition depending upon expectations of privacy, types of communications, and location of parties).
Sec. 2510(5) electronic, mechanical or other devices; (2 statutory exceptions (1) telephone or telegraph furnished in normal course of business and so used, and (2) hearing aid correcting to normal hearing).	Sec. 1526(c) eavesdropping device; deletes hearing aid as explicit exception, rephrases telephone exception, but substantially similar (note erroneous cross-reference in sec. 3108(e) to sec. 1525(c)).	Adopts title III, sec. 2510(5) definition.
Sec. 2510(6) person; individual corporations, etc.	Sec. 111 definition limits to individuals	Adopts title III, sec. 2510(6) definition; in addition there is sec. 2521(b)(9) U.S. person definition (defined as U.S. citizen, aliens lawfully admitted into United States for permanent residence, etc.). [Note lack of comma prior to last "or" of subsection is ambiguous as to whether corp. incorporated in U.S. is a separate category.]
Sec. 2510(7) investigative or law enforcement officer; Government officer empowered to investigate or arrest re: enumerated offenses (sec. 2516) and any attorney empowered to participate in prosecution.	Sec. 111 law enforcement officer definition is broader covering any public servant empowered to engage in investigation, detection, prevention, and prosecution of an offense.	Adopts title III, sec. 2510(7) definition.
Sec. 2510(8) contents	Sec. 1526(b) reworded, but substantially the same as title III (cross-reference from sec. 3108(c)).	Adopts title III, sec. 2510(8) definition; in addition there is sec. 2521(b)(5) foreign intelligence information definition.
Sec. 2510(9) judges of competent jurisdiction; any Federal district or circuit court judge and any State judge authorized by State statute.	Sec. 3108(d) court of competent jurisdiction; probably similar in effect, however, because "court" replaces "judge" ambiguous whether entire court or single judge of a court acts.	Adopts title III, sec. 2510(9) definition; however, sec. 2523 limits ch. 120 electronic surveillance jurisdiction to specifically appointed judges. [Note amendment to title III, sec. 2511(1) ambiguously uses "court" rather than "judge"].
Sec. 2510(10) communications common carrier.	Sec. 3108(b) reworded, but substantially the same as title III, sec. 2510(10) definition.	Adopts title III, sec. 2510(10) definition.
Sec. 2510(11) aggrieved person.	Sec. 3108(a) reworded, but substantially the same as title III, sec. 2510(11) definition.	Adopts title III, sec. 2510(11) definition.
Violations and exceptions:		
Sec. 2511(a) interceptions other than as provided, or use or disclosure of contents of such interception where reason to know information received by violation.	No direct analog; sec. 1521 prohibits interception without consent or disclosure of violative interception where known (higher standard of actual knowledge seems necessary, see sec. 111 reference to sec. 302(b)). [Note no explicit statement that judicial authorization under sec. 3101 acts as a defense to sec. 1521 offense; sec. 501 probably implies such]. Sec. 1521 provides greater possible imprisonment and fines than title III, Sec. 2511(1).	Title III, sec. 2511(1) (a), (c), (d) amended to include ch. 120 electronic surveillance under prohibitions.
Sec. 2511(2)(a) (i), (ii) communication common carrier exceptions.	No direct analog; sec. 1521 creates eavesdropping defense for communications common carrier and agents, etc. under similar circumstances as title III; also adds explicit language covering "supervisory service observing," but deletes specific language covering switchboard operator; sec. 3103(2)(A) covers assistance of communications common carrier to law officer provided not unlawful under title III, sec. 2511(2)(a)(ii).	Title III, sec. 2511(2)(a)(i) amended to include radio communications and all acquisitions. Title III, sec. 2511(2)(a)(ii) amended to include in exception ch. 120 electronic surveillance and in addition requires law officer to furnish judicial order or in emergency circumstances certification; if carrier provides aid before receiving documents then possible civil liability.
Sec. 2511(2)(b) FCC exemption.	No corollary found	Title III, sec. 2511(2)(b) amended to cover ch. 120 electronic surveillance.
Sec. 2511(2) (c), (d) consent	No direct analog: sec. 1521(a) description of offense excludes from offense situations where prior consent.	Title III, sec. 2511(2)(c) amended to include ch. 120 electronic surveillance (actions under color of law). Title III, sec. 2511 (2)(d) unchanged.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Title III	S. 1437	S. 1566
No corollary	No corollary	Sec. 2511(2)(e) added to provide exception allowing testing of capability of devices and determining existence of devices.
Sec. 2511(3) inherent Presidential powers.	No corollary found	Deleted; however sec. 2511(2)(f) added to provide that acquisition by other means than ch. 119 or ch. 120 are not regulated by instant provisions.
Sec. 2512 manufacture, distribution, possession, advertising, etc. of devices prohibited except for communication common carriers and government in normal course of activities including person under contract.	Secs. 1522–1523 language substantially different, but provided offenses of trafficking and possession similar to title III, as well as similar defenses; penalties, however, vary considerably from title III.	Title III, sec. 2512 unamended (arguably language broad enough to include ch. 120 electronic surveillance).
Sec. 2513 confiscation of device where violation of sec. 2511 or sec. 2512.	Sec. 4001(a)(9) authorizes forfeiture proceedings against devices where violation of secs. 1521–1523.	Title III, sec. 2513 unamended. (Note confiscation would be allowable in those situations where sec. 2511 expanded to include ch. 120; and also arguable to sec. 2512 offenses (see above)).
Sec. 2515 evidentiary usage prohibited where disclosure in violation (grand juries, courts, agencies).	Sec. 3106(a)(4) prohibits use before official proceeding of Government agency (note although sec. 111 Government agency definition seems broad there is no specific inclusion of courts through this and other parts of sec. 3106(d) suppression procedures except to extent sec. 3106(d)(3) requires court to make disclosure determination when motion before it).	Title III, sec. 2515 amended to include ch. 120 electronic surveillance in use prohibition where violation.
Authorization: Sec. 2516(1) Federal application procedure; who may apply to whom for what offenses. (Attorney general or assistant attorney general specifically designated by attorney general may authorize application by Federal agency having responsibility for and investigating of enumerated offenses to Federal judge).	Sec. 3101(a) completely reworded, but similar in effect to title III (the application procedure is substantially the same (but to "court", see above) the enumerated offenses in general delete Presidential and congressional attacks as separate categories and specific types of bribery and add arson, aircraft hijacking, and releasing classified information) (any attempt to specifically compare the offenses is futile due to S. 1437's redefinition and restructuring of the criminal code).	Title III, sec. 2516(1) unamended sec. 2522 added to institute special procedure for ch. 120 (President must preliminarily authorize, in writing, attorney general (which by sec. 2521(b)(7) definition includes an assistant attorney general specifically designated, in writing, by attorney general) to approve applications, to any of the Federal judges designated under the sec. 2523 appointment procedure); reason for application is not violation of an offense, but to seek foreign intelligence information (sec. 2521(b)(5)) of a foreign power (sec. 2521(b)(1)) or agent of a foreign power (sec. 2521(b)(2)).
Sec. 2516(2) State application procedure; who may apply to whom for what offense (where authorized by State statute principal prosecuting attorney of State or political subdivision to State judge of competent jurisdiction for enumerated types of crimes and those other dangerous ones punishable by sentences greater than 1 yr).	Sec. 3101(b) reworded but similar to title III except as to type of crimes which may be investigated by interception; gambling is deleted; dangerous crimes punishable by sentences greater than one year is deleted; conspiracies relating to listed crimes is added; violent crimes which are felonies, theft, and fraud are added if State statute allows interception for such. (Note procedure itself remains the same.)	Title III sec. 2516(2) unamended; no provisions for States to seek foreign intelligence information.
Secs. 2517(1), (2), (3), (5) disclosure and use of interceptions.	Secs. 3106(a); 3104(a), reworded and reorganized, but substantially the same in ultimate effect and procedure to title III. [Note sec. 3106(a)(1) deletes sec. 2517 (1) limitation of disclosure to another law officer; sec. 3104(a) specifically requires court to enter order on making statutory findings].	Title III, secs. 2517(1), (2), (3), (5) unamended; secs. 2526 (a), (b), (c) added to enable use and disclosure of ch. 120 electronic surveillance information for specific purposes (sec. 2521(b)(8) (A) through (F) or for criminal law enforcement (if use benefits outweight possible national security harm). [No balancing factors included].
Sec. 2517(4) privileged communications.	Sec. 3106(a)(3), reworded but same as title III, sec. 2517(4).	Title III, sec. 2517(4) unamended; sec. 2526(a) added to give same protection to ch. 120 electronic surveillance.
Sec. 2518(1) contents of application.	Sec. 3102(a) reworded but changes from title III.	Title III, sec. 2518(1) amended only to limit its application to ch. 119; sec. 2524(a), (b) added which requires application for ch. 120 to contain information in addition to what would be required under ch. 119 or S. 1437 and enables attorney general to require additional affidavits from other officers.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

93-179 O - 77 - 9

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Title III	S. 1437	S. 1566
Sec. 2518(2) judiciary authority to request additional testimony or documentary evidence.	Sec. 3102(b) gives same authority as title III.	Title III, sec. 2518(2) unamended; sec. 2524(c) added to give judicial authority to request additional information" (note unclear whether "information" broader or narrower than evidentiary authority) for ch. 120 electronic surveillance.
Sec. 2518 (3), (4) judicial order, required findings, and ordered assistance of third persons.	Sec. 3103 (a), (b) reworded, but substantially the same as title III.	Title III, secs. 2518 (3), (4) unamended except as to limiting provisions of 3d persons assistance to ch. 119; secs. 2525 (a), (b), (c) added paralleling sec. 2524 providing for judicial order contents, required findings (varying depending on whether foreign power or not) and ordered assistance of 3d persons (note language of title III, secs. 2518 (3), (4) for the most part does not necessarily restrict application to ch. 119.
Sec. 2518(5) time limitations and extensions (maximum possible 30 days before extension request).	Sec. 3103(c) reworded into positive, but same effect as title III (note deletes language that extension no longer than "judge deems necessary;" arguably this limits any judicial discretion loophole if violation claimed).	Title III, sec. 2518(5) amended only to limit application to ch. 119; sec. 2525(c) added creating similar procedure for ch. 120 but increases maximum possible time from 30 to 90 days if not foreign power and 1 yr if foreign power before extension request; specifically empowers judge to require submittal of information obtained pursuant to original order to make new findings of probable cause for extension request.
Sec. 2518(6) judicially required progress reports.	Sec. 3103(d) same in effect as title III....	Title III, sec. 2518(6) unamended, (note already specifically limited to ch. 119); no clear corollary for ch. 120 electronic surveillance to authorize judge to require periodic reports. [Note judge would seem to be able to require substance of such information where extension requested see sec. 2525(c)].
Secs. 2518(8) (a), (b) interception presentation.	Secs. 3105(a), 3106(b) same effect as title III (note however, availability or recording to court altered to "as soon as practicable" rather than "immediately"; seal prerequisite to use or disclose in official proceeding, rather than arguable reading of title III, sec. 2517 (3) invol ing disclosure only in government proceeding requires seal.	Title III, secs. 2518(8) (a), (b) unamended; no corollary for ch. 120. [Title III, secs. 2518 (a), (b) limited to ch. 119 by language.]
Sec. 2518(7) emergency situations.	Sec. 3104(b) similar to title III in procedure, but reasons for use are different (rather than determination that national security threat or conspiratorial activities, determination must be that treason, sabotage, espionage, or offense involving risk of death exists); furthermore, 48-hr period to submit application becomes maximum period rather than leeway period (standard for submittal is "as soon as practicable").	Title III, sec. 2518(7) unamended; sec. 2525(d) added to provide ch. 120 emergency situation. [Notice to judge at time of authorization by attorney general application then made "as soon as practicable" but within 24 hr; review of denial by special court under sec. 2523].
Sec. 2518(8)(c) contempt power...	No corollary found.....	Title III, 2518(8)(c) unamended; no corollary found for ch. 120 electronic surveillance.
Sec. 2518(8)(d) postemergency interception procedure notice.	Sec. 3105(b) reworded, but similar in effect to title III. [Note "person" to receive notice in singular; adds provision allow-motion for "evidence derived from such contents" which is not in title III, sec. 2518(8)(d)].	Title III, sec. 2518(8)(d) unamended; sec. 2526(d) added with similar effect for ch. 120 as title III; however, also has loophole provision under which there may be permanent failure to give notice of surveillance on showing of "good cause."
Sec. 2518(9) pretrial notice of any interception.	Sec. 3106(c) virtually the same as title III except "each party" replaced by "each aggrieved person who is a party." [Note possible implications depending on "person" definition above].	Title III sec. 2518(9) amended only to limit to ch. 119.
Sec. 2518(10)(a) suppression.....	Sec. 3106(d) analogous to title III, however, ambiguity whether sec. 3106(d)(1) language includes court proceeding; also 5 yr provision new although probably same effect as given by present 18 U.S.C. 3504. [Note sec. 2515 effect (language of sec. 2518(10)(a) indicates grant of motion per se violation)].	Title III, sec. 2518(10)(a) unamended; sec. 2526(c) allows ch. 120 suppression motions to extent allowable by present 18 U.S.C. 3504 or other statute, but if Government claims national security, review is made in camera.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

OFFICE OF THE ATTORNEY GENERAL,
Washington, D.C., March 16, 1976.

Hon. JOHN L. MCCLELLAN,
U.S. Senate, Committee on the Judiciary, Subcommittee on Criminal Laws and Procedures, Washington, D.C.

DEAR SENATOR MCCLELLAN: In your letter of March 5, 1976, you requested information concerning the experience of the Department of Justice in employing the 48 hour emergency surveillance procedure in 18 U.S.C. 2518(7), and the views of the Department with regard to the necessity or desirability of this provision. It is understood that your inquiry is prompted by the Senate Judiciary Committee's current consideration of S. 1 which in section 3104(b) carries forward section 2518(7) of current law without substantive change.

To the best of my knowledge, and according to the records of the Department of Justice, the provisions of 18 U.S.C. 2518(7) have been utilized only once by the Department. On December 9, 1975, I authorized the use of two emergency wire interceptions by the Cleveland Organized Crime Strike Force. Applications for court orders approving the interceptions were filed on December 11, 1975. The case involved the attempted extortion of $250,000 from the National Bank of Detroit, Mich., and the kidnapping and threatened murder of an assistant manager of that bank. The communications obtained by reason of the telephone interceptions played a vital role in apprehending the members of the kidnapping gang. Tragically, however, the arrests could not be made in time to prevent the death by stabbing of the kidnapping victim, the endangerment of whose life was the principal motivation for the Department's use of the emergency provisions.

In another instance, Department records show that Attorney General Saxbe authorized on March 16, 1974, the employment of an emergency interception in connection with an extortionate demand by a group seeking free radio time to publicize their views, under the threat that a hostage in their custody would be killed. Because the F.B.I. managed shortly thereafter to apprehend the members of the group, it was not necessary to implement the Attorney General's authorization and no interception occurred.

These two instances—both involving threats against the lives of hostages—represent the only occasions of which I am aware in which the Department of Justice has authorized the use of the provisions of 18 U.S.C. 2518(7).

I believe that sound reasons support the retention of the emergency provision and would therefore strongly recommend against its deletion from S. 1. The Supreme Court in other Fourth Amendment contexts has recognized that the existence of an emergency, requiring an immediate search, is justification for dispensing with the need to obtain a prior warrant from a court. For example, *Warden* v. *Hayden*, 387 U.S. 294 (1967). There is no evident reason why the same principle ought not to be applicable to searches and seizures by electronic interception.

Although I believe it is important that the emergency provision not be deleted, it may well be appropriate to attempt to redefine the types of situations described in the statute as constituting an "emergency". With regard to the coverage in 18 U.S.C. 2518(7) of "conspiratorial activities characteristic of organized crime", the statute might be refocussed on more traditional concepts justifying an "emergency" search, such as the endangerment of life and perhaps the destruction of important evidence relating to specific, highly serious offenses. There seems to be no reason why the statute should single out organized crime offenses as a proper subject for "emergency" interception, yet omit instances in which human life may be imperiled though the criminal actions of one or more persons under conditions that are not characteristic of organized crime. With regard to the present section's coverage of "conspiratorial activities affecting the national security interest", such cases, although they might not involve an immediate danger to human life, may often involve an eventual danger to many lives. Acts of treason, sabotage, and espionage may control the outcome of wars. Such situations should continue to be covered by the exception, although a more particularized definition could be considered.

In short, I believe that the existence of an "emergency" provision—even though seldom used—is important and justified in both legal principle and practical policy, but that the focus of the provision on organized criminal conspiracies might appropriately be shifted to more traditional notions of emergency.

Sincerely,

EDWARD H. LEVI.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

COMMON CAUSE,
Washington, D.C., June 24, 1977.

Hon. JOHN L. MCCLELLAN,
Chairman, Senate Judiciary Subcommittee on Criminal Laws and Procedures, Dirksen Office Building, Washington, D.C.

DEAR MR. CHAIRMAN: We are enclosing our statement on S. 1566, the "Foreign Intelligence Surveillance Act of 1977," for inclusion in the Committee's hearing record on this legislation.

Sincerely,

DAVID COHEN, *President.*

COMMON CAUSE STATEMENT ON "FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1977," S. 1566

Common Cause appreciates this opportunity to submit our comments on S. 1566, the Foreign Intelligence Surveillance Act of 1977. We are especially pleased that wiretaping for intelligence purposes is receiving consideration in this session. While we firmly believe it is time for Congress to establish the law and limits on such wiretaps, our particular concern with the bill before you is the authority it would give to conduct electronic surveillance of persons not suspected of criminal activity.

As others have testified, wiretaps are the most intrusive and least precise means of gathering relevant information. All conversations on a telephone are heard, whether or not the speakers are the targets of the surveillance. In addition, it is impossible to limit the interception to conversations that are relevant to the purposes for which the tap is placed. Consequently, personal information, trivial information, gossip and, significantly, purely political information can be gathered. The intrusive and chilling effect of wiretaps was well-documented in the Senate Select Intelligence Committee's report on domestic electronic surveillance. We know that political information can be gathered, because it has been. We are aware that trivialities can be garnered, because they were. What we don't know is whether any useful information has ever been gleaned from wiretaps. We assume it has.

The abuses in the name of national security that have been uncovered in the past few years make it imperative that this Congress deal with the many questions on national security wiretaps currently left unanswered in the law. We believe that the bill before this committee is an improvement over its predecessor —S. 3197 in the 94th Congress—in that it rejects any asertion of an inherent Presidential power to conduct wiretaps. That was one of the main objections raised against S. 3197 last year by Common Cause and others, and we are pleased that it has not been included in S. 1566.

Another of our principal concerns remains, however, and that is the lack of a criminal standard for all wiretaps. We believe that the absence of a criminal standard is a fundamental flaw in the bill which must be remedied.

S. 1566 would authorize wiretaps for 90 days or more of at least four classes of persons who are not engaged in any criminal activity: officers or employees of a foreign power; foreigners engaged in undefined "clandestine intelligence activities" which may be harmful to the national security; Americans who secretly collect or transmit information pursuant to the direction of a foreign intelligence service where such collection or transmission would be harmful to the national security; and persons who knowingly aid or abet others in undefined clandestine intelligence activities or the secret transmission or collection of harmful information.

The amply-documented abuses which were executed under the guise of national security should warn us of the need to proceed cautiously, if at all, before legitimizing wiretapping without the need to prove probable criminal activity. As the final report of the Church Committee stated, "Targeting an American for electronic surveillance in the absence of probable cause to believe he might commit a crime is unwise and unnecessary." ("Intelligence Activities and The Right of Americans," Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Book II, U.S. Senate, 94th Cong., 2d Sess., at 325.) If our espionage laws are insufficient to cover modern forms of industrial, technological or economic espionage, then the proper course is to amend those laws, not to permit wiretapping on less than a criminal standard. We fully agree with the Church Committee's judgment that—

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

"* * * as a matter of principle, * * * an American ought not to be targeted for surveillance unless there is probable cause to believe he may violate the law. The Committee's record suggests that use of undefined terms, not tied to matters sufficiently serious to be the subject of criminal statutes, is a dangerous basis for intrusive investigations" (Final Report, at 325).

The Rockefeller Commission reached essentially the same conclusion with reference to wiretaps conducted by the CIA. In its final report to the President, it recommended that the CIA not be permitted to collect information about the domestic activities of U.S. citizens by either covert or overt means with four exceptions, one of which was "Persons suspected of espionage or other illegal activities relating to foreign intelligence * * *" (Report to the President by the Commission on CIA Activities within the United States, June 1975, p. 13.) While the Commission's recommendations are directed at the CIA, they are relevant to a discussion of S. 1566 because of the recognition by the Commission of the need for a connection between illegal activities and covert surveillance.

In our view, the fourth amendment and its prohibition that "no warrants shall issue, but upon probable cause * * *" would appear to mandate a criminal standard for all wiretaps. If Congress does not see fit to make certain activities criminal, then we see no reason to permit this highly intrusive form of search with all its dragnet effects.

We have seen the extent to which the words "national security" have been stretched far beyond reasonable limits. Circumvention of the fourth amendment in the name of "national security" alone is opening the door to the erosion of our first amendment rights. The people's right to be free from Government surveillance is inextricably bound up with their rights of free speech, press, and association. In the absence of probable criminal activity, there is no justification for permitting the chilling effect brought about by the mere possibility of wiretapping. Americans should be free to act in ways which Congress has not made illegal without fear of Government surveillance.

The significance of the criminal standard also goes beyond the confines of this bill. If the FBI is given explicit authority to place wiretaps on persons not suspected of criminal activity, what is to stop it from assuming that other forms of investigations may also be carried out without any connection to probable criminal activity? Instead of implicitly permitting or encouraging that result, we should be working to end, once and for all, the possibility of the recurrence of abuses which have been uncovered in recent years—the CIA's mail-openings; IRS selective auditing on the basis of White House politics; the FBI's COINTELPRO program and its black bag jobs. The first piece of legislation to be considered in the wake of past intelligence agency abuses must firmly establish that investigations and other activities must not be carried out on the basis of noncriminal "national security" grounds.

We hope that as the committee considers the critical issue of what standard must be met before electronic surveillance may be carried out, it will reject the provisions in the present bill and insist upon a criminal standard.

PREPARED STATEMENT OF WOMEN STRIKE FOR PEACE

Women Strike for Peace (WSP), a women's movement started in 1961 in response to the dangers from nuclear atmospheric tests and world tensions, is dedicated to the achievement of world peace through general and complete disarmament with international controls. Women Strike for Peace is opposed to S. 1566 because we are against any and all electronic surveillance against individuals. We consider wiretapping or bugging an abrogation of the most basic constitutional rights provided by the fourth amendment. It is also the most intrusive invasion of the privacy of the individual.

WSP's strong opposition to S. 1566 is also based on our own experience with the Intelligence Agencies. It was the Rockefeller Commission which revealed in 1975 that WSP was infiltrated and spied upon by the CIA during their "Operation Chaos." An examination of files made available through the Freedom of Information Act revealed that WSP's activities were also monitored by the FBI, the Army, the Air Force and the State Dept. These were the federal agencies charged with law enforcement and protection of our national security, who themselves engaged in illegal, unconstitutional activities—disrupting constitutionally protected activities of women. Government spying on organizations and indi-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

93-179 O - 77 - 10

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

viduals for political dissent is not effectively stopped by S. 1566. In fact, the use of a "noncriminal standard" will make it easier for intelligence gathering agencies to continue the abuses of constitutional rights.

S. 1566 would, for the first time in American peacetime history, legitimize wiretapping solely for the purpose of gaining information about undefined and unspecified "clandestine intelligence activities." The broad definitions in S. 1566 for "foreign power," "agent of a foreign power" and "foreign intelligence information" is a stark reminder of the recent abuses by the intelligence agencies who used "foreign domination" as their rationale. S. 1566 would inhibit Americans from exercising their constitutional right to make contacts with people from foreign countries and benefit from independent sources of information. Otherwise, citizens are totally dependent on official sources and are therefore deprived of their democratic right to arrive at decisions autonomously. Leaders, instead of expressing the will of the people, are given the power to dictate that will. Citizen to citizen exchange should be encouraged, not made suspect. WSP believes that such contact helps develop better understanding and better relations between peoples of all countries. We in WSP have established this policy from our beginning. We've met with women from many countries including the socialist countries.

We think it is ironic that while President Carter is moving to open up new contacts, new exchanges in foreign policy, S. 1566 would make these exchanges a basis for wiretapping.

We are also concerned that acceptance of a warranting procedure for electronic surveillance unrelated to crime establishes an alarming precedent. This legislation may be followed by legislation seeking a warrant procedure for mail openings and "surreptitious entries" unrelated to crime. The result may be to legitimize all of the techniques illegaly employed in the past.

AMERICAN ETHICAL UNION,
June 9, 1977.

CHIEF COUNSEL,
Senate Judiciary Committee,
Washingon, D.C.

DEAR SIR: I respectfully request that the enclosed statement be entered into the hearings record on S. 1566.

I would also appreciate it very much if a copy of the hearings record could be sent to me when it is printed.

Sincerely,

RAYMOND NATHAN,
Director, Washington Ethical Action Office.

PREPARED STATEMENT OF RAYMOND NATHAN, DIRECTOR, WASHINGTON ETHICAL ACTION OFFICE, AMERICAN ETHICAL UNION

As a federation of religious bodies which find their highest value in human worth, the American Ethical Union is seriously troubled by S. 1566 in its present form.

While the bill does not support the pernicious doctrine of inherent presidential power to commit otherwise illegal acts, its net practical effect could be just that. By allowing the President to get a court order for electronic surveillance of an American citizen to seek information related to "the succesful conduct of the foreign affairs of the United States," the door is left open for the kind of wiretapping of journalists and social activities which took place under President Nixon. Americans were shocked and repelled when this was revealed, because it meant that their treasured right of privacy, which they thought was protected by the Fourth Amendment, was not safe from government intrusion.

In 1974 and 1976, annual assemblies of the American Ethical Union passed resolutions against the wiretapping provisions in S. 1400 and S. 1. It is regrettable that in 1977, when we had hoped government would demonstrate greater respect for the rights of the individual, the Administration and several distinguished Senators are calling for a bill that would seriously diminish those rights.

We hope that in its work on S. 1566 the Committee will keep in mind the recommendation of the Senate Select Committee on Intelligence Activities that "no American be targeted for electronic surveillance except upon a judicial finding of probable criminal activity."

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

95TH CONGRESS
1ST SESSION

S. 1566

IN THE SENATE OF THE UNITED STATES

MAY 18 (legislative day, MAY 16), 1977

Mr. KENNEDY (for himself, Mr. BAYH, Mr. EASTLAND, Mr. INOUYE, Mr. MCCLELLAN, Mr. MATHIAS, Mr. NELSON, and Mr. THURMOND) introduced the following bill; which was read twice and referred by unanimous consent to the Committee on the Judiciary, and, if and when reported, then to the Select Committee on Intelligence

A BILL

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*
3 That this Act may be cited as the "Foreign Intelligence
4 Surveillance Act of 1977".
5 SEC. 2. Title 18, United States Code, is amended by
6 adding a new chapter after chapter 119 as follows:

II

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 **"Chapter 120.—ELECTRONIC SURVEILLANCE WITH-**
2 **IN THE UNITED STATES FOR FOREIGN INTEL-**
3 **LIGENCE PURPOSES**

"Sec.
"2521. Definitions.
"2522. Authorization for electronic surveillance for foreign intelligence purposes.
"2523. Designation of judges authorized to grant orders for electronic surveillance.
"2524. Application for an order.
"2525. Issuance of an order.
"2526. Use of information.
"2527. Report of electronic surveillance."

4 **"§ 2521. Definitions**

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

8 "(b) As used in this chapter—

9 "(1) 'Foreign power' means—

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

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

15 "(C) an entity, which is openly acknowledged
16 by a foreign government or governments to be
17 directed and controlled by such foreign government
18 or governments;

19 "(D) a foreign-based terrorist group;

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(E) a foreign-based political organization, not
2 substantially composed of United States persons; or
3 "(F) an entity which is directed and controlled
4 by a foreign government or governments.
5 "(2) 'Agent of a foreign power' means—
6 "(A) any person, other than a United States
7 citizen or an alien lawfully admitted for perma-
8 nent residence (as defined in section 101 (a) (20)
9 of the Immigration and Nationality Act), who—
10 "(i) is an officer or employee of a foreign
11 power;
12 "(ii) knowingly engages in clandestine
13 intelligence activities for or on behalf of a
14 foreign power under circumstances which in-
15 dicate that such activities would be harmful to
16 the security of the United States; or
17 "(iii) conspires with or knowingly aids
18 or abets a person described in paragraph (ii)
19 above;
20 "(B) any person who—
21 "(i) knowingly engages in clandestine
22 intelligence activities for or on behalf of a for-
23 eign power, which activities involve or will

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 involve a violation of the criminal statutes of
2 the United States;
3 "(ii) knowingly engages in activities that
4 involve or will involve sabotage or terrorism
5 for or on behalf of a foreign power;
6 "(iii) pursuant to the direction of an intel-
7 ligence service or intelligence network of a
8 foreign power, knowingly collects or transmits
9 information or material to an intelligence service
10 or intelligence network of a foreign power in a
11 manner intended to conceal the nature of such
12 information or material or the fact of such
13 transmission or collection, under circumstances
14 which indicate the transmission of such informa-
15 tion or material would be harmful to the security
16 of the United States, or that lack of knowledge
17 by the United States of such collection or trans-
18 mission would be harmful to the security of the
19 United States; or
20 "(iv) conspires with or knowingly aids or
21 abets any person engaged in activities described
22 in subsections B (i) or (iii) above.
23 "(3) 'Terrorism' means activities which—
24 "(A) are violent acts or acts dangerous to
25 human life which would be criminal under the laws

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

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;

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(C) information which relates to, and is
2 deemed necessary to the ability of the United
3 States to protect against terrorism by a foreign
4 power or an agent of a foreign power;
5 "(D) information which relates to, and is
6 deemed necessary to the ability of the United States
7 to protect against sabotage by a foreign power or
8 an agent of a foreign power; or
9 "(E) information which relates to, and is
10 deemed necessary to the ability of the United States
11 to protect against the clandestine intelligence activi-
12 ties of an intelligence service or network of a foreign
13 power or an agent of a foreign power.
14 "(6) 'Electronic surveillance' means—
15 "(A) the acquisition by an electronic, me-
16 chanical, or other surveillance device of the con-
17 tents of any wire or radio communication sent by
18 or intended to be received by a particular, known
19 United States person who is in the United States,
20 where the contents are acquired by intentionally
21 targeting that United States person, under circum-
22 stances in which a person has a reasonable expecta-
23 tion of privacy and a warrant would be required for
24 law enforcement purposes;
25 "(B) the acquisition by an electronic, mechan-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 ical, or other surveillance device, of the contents of
2 any wire communication to or from a person in the
3 United States, without the consent of any party
4 thereto, where such acquisition occurs in the United
5 States while the communication is being trans-
6 mitted by wire;
7 "(C) the intentional acquisition, by an elec-
8 tronic, mechanical, or other surveillance device, of
9 the contents of any radio communication, under
10 circumstances in which a person has a reasonable
11 expectation of privacy and a warrant would be
12 required for law enforcement purposes, and where
13 both the sender and all intended recipients are
14 located within the United States; or
15 "(D) the installation or use of an electronic,
16 mechanical, or other surveillance device in the
17 United States for monitoring to acquire information,
18 other than from a wire or radio communication,
19 under circumstances in which a person has a reason-
20 able expectation of privacy and a warrant would be
21 required for law enforcement purposes.
22 "(7) 'Attorney General' means the Attorney Gen-
23 eral of the United States (or Acting Attorney General)
24 or an Assistant Attorney General specially designated in
25 writing by the Attorney General.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(8) 'Minimization procedures' means procedures
2 which are reasonably designed to minimize the acquisi-
3 tion, retention, and dissemination of any information
4 concerning United States persons without their consent
5 that does not relate to the ability of the United States—
6 "(A) to protect itself against actual or potential
7 attack or other grave hostile acts of a foreign power
8 or an agent of a foreign power;
9 "(B) to provide for the national defense or
10 security of the Nation;
11 "(C) to provide for the conduct of the foreign
12 affairs of the United States;
13 "(D) to protect against terrorism by a foreign
14 power or an agent of a foreign power;
15 "(E) to protect against sabotage by a foreign
16 power or an agent of a foreign power; or
17 "(F) to protect against the clandestine in-
18 telligence activities of an intelligence service or
19 network of a foreign power or an agent of a foreign
20 power;
21 and which are reasonably designed to insure that infor-
22 mation which relates solely to the conduct of foreign
23 affairs shall not be maintained in such a manner as to
24 permit the retrieval of such information by reference to a
25 United States person, without his consent, who was a

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 party to a communication acquired pursuant to this
2 chapter; and if the target of the electronic surveillance
3 is a foreign power which qualifies as such solely on the
4 basis that it is an entity controlled and directed by a
5 foreign government or governments, and unless there is
6 probable cause to believe that a substantial number of
7 the officers or executives of such entity are officers or
8 employees of a foreign government, or agents of a for-
9 eign power as defined in section 2521 (b) (2) (B), pro-
10 cedures which are reasonably designed to prevent the
11 acquisition, retention, and dissemination of communica-
12 tions of unconsenting United States persons who are not
13 officers or executives of such entity responsible for those
14 areas of its activities which involve foreign intelligence
15 information.

16 "(9) 'United States person' means a citizen of the
17 United States, an alien lawfully admitted for permanent
18 residence (as defined in section 101 (a) (20) of the
19 Immigration and Nationality Act), an unincorporated
20 association a substantial number of members of which are
21 citizens of the United States or aliens lawfully admitted
22 for permanent residence or a corporation which is incor-
23 porated in the United States, but not including corpora-
24 tions which are foreign powers.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(10) 'United States' when used in a geographic
2 sense means all areas under the territorial sovereignty of
3 the United States, the Trust Territory of the Pacific Is-
4 lands, and the Canal Zone.

5 **"§ 2522. Authorization for electronic surveillance for for-**
6 **eign intelligence purposes**

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

16 **"§ 2523. Designation of judges authorized to grant orders**
17 **for electronic surveillance**

18 "(a) The Chief Justice of the United States shall pub-
19 licly designate seven district court judges, each of whom
20 shall have jurisdiction to hear applications for and grant
21 orders approving electronic surveillance anywhere within
22 the United States under the procedures set forth in this chap-
23 ter, except that no judge designated under this subsection
24 shall have jurisdiction of the same application for electronic
25 surveillance under this chapter which has been denied previ-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 ously by another judge designated under this subsection. If
2 any judge so designated denies an application for an order
3 authorizing electronic surveillance under this chapter, such
4 judge shall provide immediately for the record a written
5 statement of each reason for his decision and, on motion of
6 the United States, the record shall be transmitted, under
7 seal, to the special court of review established in subsec-
8 tion (b).

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

21 "(c) Proceedings under this chapter shall be conducted
22 as expeditiously as possible. The record of proceedings under
23 this chapter, including applications made and orders granted,
24 shall be sealed and maintained under security measures estab-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 lished by the Chief Justice in consultation with the Attorney
2 General and the Director of Central Intelligence.
3 **"§ 2524. Application for an order**
4 "(a) Each application for an order approving electronic
5 surveillance under this chapter shall be made by a Federal
6 officer in writing upon oath or affirmation to a judge having
7 jurisdiction under section 2523 of this chapter. Each appli-
8 cation shall require the approval of the Attorney General
9 based upon his finding that it satisfies the criteria and require-
10 ments of such application as set forth in this chapter. It shall
11 include the following information—
12 "(1) the identity of the Federal officer making the
13 application;
14 "(2) the authority conferred on the Attorney Gen-
15 eral by the President of the United States and the ap-
16 proval of the Attorney General to make the application;
17 "(3) the identity or a description of the target of
18 the electronic surveillance;
19 "(4) a statement of the facts and circumstances
20 relied upon by the applicant to justify his belief that—
21 "(A) the target of the electronic surveillance
22 is a foreign power or an agent of a foreign power;
23 and
24 "(B) the facilities or the place at which the
25 electronic surveillance is directed are being used,

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 or are about to be used, by a foreign power or an
2 agent of a foreign power;
3 "(5) a statement of the proposed minimization
4 procedures;
5 "(6) when the target of the surveillance is not
6 a foreign power as defined in section 2521 (b) (1) (A),
7 (B) or (C), a detailed description of the nature of the
8 information sought;
9 "(7) a certification or certifications by the Assist-
10 ant to the President for National Security Affairs or an
11 executive branch official or officials designated by the
12 President from among those executive officers employed
13 in the area of national security or defense and appointed
14 by the President with the advice and consent of the
15 Senate—
16 "(A) that the information sought is foreign
17 intelligence information;
18 "(B) that the purpose of the surveillance is
19 to obtain foreign intelligence information;
20 "(C) that such informaton cannot reasonably
21 be obtained by normal investigative techniques;
22 "(D) including a designation of the type of
23 foreign intelligence information being sought accord-
24 ing to the categories described in section 2521
25 (b) (5);

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(E) when the target of the surveillance is not
2 a foreign power, as defined in section 2521 (b) (1)
3 (A), (B), or (C), including a statement of the
4 basis for the certification that—
5 "(i) the information sought is the type
6 of foreign intelligence information designated;
7 and
8 "(ii) such information cannot reasonably
9 be obtained by normal investigative techniques;
10 "(F) when the target of the surveillance is
11 a foreign power, as defined in section 2521 (b) (1)
12 (A), (B), or (C), stating the period of time for
13 which the surveillance is required to be maintained;
14 "(8) when the target of the surveillance is not
15 a foreign power, as defined in section 2521 (b) (1)
16 (A), (B), or (C), a statement of the means by which
17 the surveillance will be effected, and when the target is
18 a foreign power, as defined in section 2521 (b) (1)
19 (A), (B), or (C), a designation of the type of elec-
20 tronic surveillance to be used according to the categories
21 described in section 2521 (b) (6);
22 "(9) a statement of the facts concerning all previous
23 applications that have been made to any judge under
24 this chapter involving any of the persons, facilities, or

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 places specified in the application, and the action taken
2 on each previous application; and
3 "(10) when the target of the surveillance is not a
4 foreign power, as defined in section 2521 (b) (1) (A),
5 (B), or (C), a statement of the period of time for which
6 the electronic surveillance is required to be maintained.
7 If the nature of the intelligence gathering is such that
8 the approval of the use of electronic surveillance under
9 this chapter should not automatically terminate when
10 the described type of information has first been obtained,
11 a description of facts supporting the belief that addi-
12 tional information of the same type will be obtained
13 thereafter.
14 "(b) The Attorney General may require any other
15 affidavit or certification from any other officer in connection
16 with the application.
17 "(c) The judge may require the applicant to furnish
18 such other information as may be necessary to make the
19 determinations required by section 2525 of this chapter.
20 **"§ 2525. Issuance of an order**
21 "(a) Upon an application made pursuant to section
22 2524 of this title, the judge shall enter an ex parte order as
23 requested or as modified approving the electronic surveil-
24 lance if he finds that—

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4
93-179 O - 77 - 11

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(1) the President has authorized the Attorney
2 General to approve applications for electronic surveil-
3 lance for foreign intelligence information;
4 "(2) the application has been made by a Federal
5 officer and approved by the Attorney General;
6 "(3) on the basis of the facts submitted by the
7 applicant there is probable cause to believe that—
8 "(A) the target of the electronic surveillance
9 is a foreign power or an agent of a foreign power;
10 and
11 "(B) the facilities or place at which the elec-
12 tronic surveillance is directed are being used, or
13 are about to be used, by a foreign power or an agent
14 of a foreign power;
15 "(4) the proposed minimization procedures meet
16 the definition of minimization procedures under section
17 2521 (b) (8) of this title;
18 "(5) the application which has been filed contains
19 the description and certification or certifications, spec-
20 ified in section 2524 (a) (7) and, if the target is a
21 United States person, the certification or certifications
22 are not clearly erroneous on the basis of the statement
23 made under section 2524 (a) (7) (E).
24 "(b) An order approving an electronic surveillance
25 under this section shall—

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(1) specify—
2 "(A) the identity or a description of the target
3 of the electronic surveillance;
4 "(B) the nature and location of the facilities or
5 the place at which the electronic surveillance will be
6 directed;
7 "(C) the type of information sought to be
8 acquired;
9 "(D) when the target of the surveillance is not
10 a foreign power, as defined in section 2521 (b) (1)
11 (A), (B), or (C), the means by which the elec-
12 tronic surveillance will be effected, and when the tar-
13 get is a foreign power, as defined in section 2521 (b)
14 (1) (A), (B), or (C), a designation of the type
15 of electronic surveillance to be used according to the
16 categories described in section 2521 (b) (6); and
17 "(E) the period of time during which the elec-
18 tronic surveillance is approved; and
19 "(2) direct—
20 "(A) that the minimization procedures be
21 followed;
22 "(B) that, upon the request of the applicant, a
23 specified communication or other common carrier,
24 landlord, custodian, contractor, or other specified
25 person furnish the applicant forthwith any and all

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 information, facilities, or technical assistance, neces-
2 sary to accomplish the electronic surveillance in such
3 manner as will protect its secrecy and produce a
4 minimum of interference with the services that such
5 carrier, landlord, custodian, contractor, or other per-
6 son is providing that target of electronic surveillance;
7 "(C) that such carrier, landlord, custodian, or
8 other person maintain under security procedures
9 approved by the Attorney General and the Direc-
10 tor of Central Intelligence any records concerning
11 the surveillance or the aid furnished which such
12 person wishes to retain;
13 "(D) that the applicant compensate, at the
14 prevailing rate, such carrier, landlord, custodian, or
15 other person for furnishing such aid.
16 "(c) An order issued under this section may approve
17 an electronic surveillance not targeted against a foreign
18 power, as defined in section 2521(b)(1) (A), (B), or
19 (C), for the period necessary to achieve its purpose, or for
20 ninety days, whichever is less; an order under this section
21 shall approve an electronic surveillance targeted against a
22 foreign power, as defined in section 2521(b)(1) (A),
23 (B), or (C) for the period specified in the certification
24 required in section 2524(a)(7)(F), or for one year, which-
25 ever is less. Extensions of an order issued under this chapter

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 may be granted on the same basis as an original order upon
2 an application for an extension made in the same manner
3 as required for an original application and after new find-
4 ings required by subsection (a) of this section. In connec-
5 tion with applications for extensions where the target is not
6 a foreign power, as defined in section 2521 (b) (1) (A),
7 (B), or (C), the judge may require the applicant to sub-
8 mit information, obtained pursuant to the original order or
9 to any previous extensions, as may be necessary to make
10 new findings of probable cause.
11 "(d) Notwithstanding any other provision of this chap-
12 ter when the Attorney General reasonably determines
13 that—
14 "(1) an emergency situation exists with respect to
15 the employment of electronic surveillance to obtain for-
16 eign intelligence information before an order authorizing
17 such surveillance can with due diligence be obtained,
18 and
19 "(2) the factual basis for issuance of an order under
20 this chapter to approve such surveillance exists, he may
21 authorize the emergency employment of electronic sur-
22 veillance if a judge designated pursuant to section 2523
23 of this chapter is informed by the Attorney General or
24 his designate at the time of such authorization that the
25 decision has been made to employ emergency electronic

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 surveillance and if an application in accordance with this
2 chapter is made to that judge as soon as practicable, but
3 not more than twenty-four hours after the Attorney
4 General authorizes such acquisition. If the Attorney
5 General authorizes such emergency employment of elec-
6 tronic surveillance, he shall require that the minimization
7 procedures required by this chapter for the issuance of
8 a judicial order be followed. In the absence of a judicial
9 order approving such electronic surveillance, the surveil-
10 lance shall terminate when the information sought is
11 obtained, when the application for the order is denied,
12 or after the expiration of twenty-four hours from the
13 time of authorization by the Attorney General, which-
14 ever is earliest. In the event that such application for
15 approval is denied, or in any other case where the elec-
16 tronic surveillance is terminated without an order hav-
17 ing been issued, no information obtained or evidence
18 derived from such surveillance shall be received in evi-
19 dence or otherwise disclosed in any trial, hearing or
20 other proceeding in or before any court, grand jury,
21 department, office, agency, regulatory body, legislative
22 committee or other authority of the United States, a
23 State or political subdivision thereof. A denial of the
24 application made under this subsection may be reviewed
25 as provided in section 2523.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 **"§ 2526. Use of information**

2 "(a) Information concerning United States persons
3 acquired from an electronic surveillance conducted pursuant
4 to this chapter may be used and disclosed by Federal officers
5 and employees without the consent of the United States per-
6 son only for purposes specified in section 2521 (b) (8) (A)
7 through (F), or for the enforcement of the criminal law if
8 its use outweighs the possible harm to the national security.
9 No otherwise privileged communication obtained in accord-
10 ance with, or in violation of, the provisions of this chapter
11 shall lose its privileged character.

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

19 "(c) Whenever the Government intends to enter into
20 evidence or otherwise use or disclose in any trial, hearing,
21 or other proceeding in or before any court, department,
22 officer, agency, or other authority of the United States, any
23 information obtained or derived from an electronic surveil-
24 lance, the Government shall prior to the trial, hearing, or
25 other proceeding or at a reasonable time prior to an effort

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 to so disclose or so use the information or submit it in evi-
2 dence notify the court in which the information is to be
3 disclosed or used or, if the information is to be disclosed or
4 used in or before another authority, shall notify a court in
5 the district wherein the information is to be so disclosed or so
6 used that the Government intends to so disclose or so use
7 such information. Whenever any court is so notified, or
8 whenever a motion is made pursuant to section 3504 of
9 this title, or any other statute or rule of the United States
10 to suppress evidence on the grounds that it was obtained or
11 derived from an unlawful electronic surveillance, the court,
12 or where the motion is made before another authority, a
13 court in the same district as the authority, shall notwith-
14 standing any other law, if the Government by affidavit asserts
15 that an adversary hearing would harm the national security
16 or the foreign affairs of the United States, review in camera
17 and ex parte the application, order, and so much of the
18 transcript of the surveillance as may be necessary to deter-
19 mine whether the surveillance was authorized and conducted
20 in a manner that did not violate any right afforded by the
21 Constitution and statutes of the United States to the person
22 aggrieved: *Provided,* That in making this determination, the
23 court shall disclose to the aggrieved person portions of the
24 application, order, or transcript only where such disclosure is
25 necessary for an accurate determination of the legality of the

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 surveillance. If the court determines that the electronic sur-
2 veillance of the person aggrieved was not lawfully authorized
3 or conducted, the court shall in accordance with the require-
4 ments of law suppress that information which was obtained
5 or evidence derived unlawfully from the electronic surveil-
6 lance of the person aggrieved.

7 "(d) If an emergency employment of the electronic
8 surveillance is authorized under section 2525(d) and a sub-
9 sequent order approving the surveillance is not obtained, the
10 judge shall cause to be served on any United States person
11 named in the application and on such other United States
12 persons subject to electronic surveillance as the judge may
13 determine in his discretion it is in the interest of justice to
14 serve, notice of—

15 "(1) the fact of the application;

16 "(2) the period of the surveillance; and

17 "(3) the fact that during the period information
18 was or was not obtained.

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

25 **"§ 2527. Report of electronic surveillance**

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "In April of each year, the Attorney General shall
2 report to the Administrative Office of the United States
3 Courts and shall transmit to Congress with respect to the
4 preceding calendar year—
5 "(1) the total number of applications made for
6 orders and extensions of orders approving electronic
7 surveillance; and
8 "(2) the total number of such orders and extensions
9 either granted, modified, or denied.".
10 SEC. 3. The provisions of this Act and the amendment
11 made hereby shall become effective upon enactment: *Pro-*
12 *vided,* That any electronic surveillance approved by the
13 Attorney General to gather foreign intelligence information
14 shall not be deemed unlawful for failure to follow the proce-
15 dures of chapter 120, title 18, United States Code, if that
16 surveillance is terminated or an order approving that surveil-
17 lance is obtained under this chapter within ninety days fol-
18 lowing the designation of the first judge pursuant to section
19 2523 of chapter 120, title 18, United States Code.
20 SEC. 4. Chapter 119 of title 18, United States Code, is
21 amended as follows:
22 (a) Section 2511 (1) is amended—
23 (1) by inserting "or chapter 120 or with respect
24 to techniques used by law enforcement officers not in-
25 volving the interception of wire or oral communications

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

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

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

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

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

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

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

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

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 (2) Section 2511 (2) (a) (ii) is amended by inserting
2 the words "or chapter 120" after the second appearance of
3 the word "chapter," and by striking the period at the end
4 thereof and adding the following: "or engage in electronic
5 surveillance, as defined in chapter 120: *Provided, however,*
6 That before the information, facilities, or technical assistance
7 may be provided, the investigative or law enforcement officer
8 shall furnish to the officer, employee, or agent of the carrier
9 either—
10 "(1) an order signed by the authorizing judge
11 certifying that a court order directing such assistance has
12 been issued; or
13 "(2) in the case of an emergency interception or
14 electronic surveillance as provided for in section 2518
15 (7) of this chapter or section 2525 (d) of chapter 120,
16 a certification under oath by investigative or law en-
17 forcement officer that the applicable statutory require-
18 ments have been met,
19 and setting forth the period of time for which the electronic
20 surveillance is authorized and describing the facilities from
21 which the communication is to be acquired. Any violation
22 of this subsection by a communication common carrier or an
23 officer, employee, or agency thereof, shall render the carrier
24 liable for the civil damages provided for in section 2520.".
25 (c) (1) Section 2511 (2) (b) is amended by inserting

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 the words "or otherwise engage in electronic surveillance, as
2 defined in chapter 120," after the word "radio".
3 (2) Section 2511 (2) (c) is amended by inserting the
4 words "or engage in electronic surveillance, as defined in
5 chapter 120," after the words "oral communication" and by
6 inserting the words "or such surveillance" after the last word
7 in the paragraph and before the period.
8 (3) Section 2511 (2) is amended by adding at the end
9 of the section the following provisions:
10 "(e) Notwithstanding any other provision of this title
11 or sections 605 or 606 of the Communications Act of 1934,
12 it shall not be unlawful for an officer, employee, or agent of
13 the United States in the normal course of his official duty to
14 conduct electronic surveillance as defined in section 2521
15 (b) (6) of chapter 120 without a court order for the sole
16 purpose of:
17 "(i) testing the capability of electronic equipment,
18 provided that the test period shall be limited in extent
19 and duration to that necessary to determine the capabil-
20 ity of the equipment, that the content of any communica-
21 tion acquired under this paragraph shall be retained
22 and used only for the purpose of determining the ca-
23 pability of such equipment, shall be disclosed only to the
24 persons conducting the test, and shall be destroyed upon
25 completion of the testing, and that the test may exceed

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 ninety days only with the prior approval of the Attorney
2 General; or
3 "(ii) determining the existence and capability of
4 electronic surveillance equipment being used unlawfully,
5 provided that such electronic surveillance shall be lim-
6 ited in extent and duration to that necessary to deter-
7 mine the existence and capability of such equipment,
8 and that any information acquired by such surveillance
9 shall be used only to enforce this chapter or section 605
10 of the Communications Act of 1934 or to protect infor-
11 mation from unlawful electronic surveillance.
12 "(f) Nothing contained in this chapter, or section 605
13 of the Communications Act of 1934 (47 U.S.C. 605) shall
14 be deemed to affect the acquisition by the United States
15 Government of foreign intelligence information from inter-
16 national communications by a means other than electronic
17 surveillance as defined in section 2521 (b) (6) of this title;
18 and the procedures in this chapter and chapter 120 of this
19 title, shall be the exclusive means by which electronic sur-
20 veillance, as defined in section 2521 (b) (6) of chapter 120,
21 and the interception of domestic wire and oral communica-
22 tions may be conducted.".
23 (d) Section 2511 (3) is repealed.
24 (e) Section 2515 is amended by inserting the words
25 "or electronic surveillance, as defined in chapter 120, has
26 been conducted" after the word "intercepted", by inserting

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 the words "or other information obtained from electronic
2 surveillance, as defined in chapter 120," after the second
3 appearance of the word "communication", and by inserting
4 "or chapter 120" after the final appearance of the word
5 "chapter".

6 (f) Section 2518 (1) is amended by inserting the words
7 "under this chapter" after the word "communication".

8 (g) Section 2518 (4) is amended by inserting the words
9 "under this chapter" after both appearances of the words
10 "wire or oral communication".

11 (h) Section 2518 (9) is amended by striking the word
12 "intercepted" and inserting the words "intercepted pursuant
13 to this chapter" after the word "communication".

14 (i) Section 2519 (3) is amended by inserting the words
15 "pursuant to this chapter" after the words "wire or oral
16 communications" and after the words "granted or denied".

17 (j) Section 2520 is amended by deleting all before
18 subsection (2) and inserting in lieu thereof: "Any person
19 other than a foreign power or an agent of a foreign power
20 as defined in sections 2521 (b) (1) and 2521 (b) (2) (A)
21 of chapter 120, who has been subject to electronic surveil-
22 lance, as defined in chapter 120, or whose wire or oral com-
23 munication has been intercepted, or about whom informa-
24 tion has been disclosed or used, in violation of this chapter,
25 shall (1) have a civil cause of action against any person
26 who so acted in violation of this chapter and".

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Calendar No. 643

95TH CONGRESS
2D SESSION

S. 1566

[Report No. 95-604]

[Report No. 95-701]

IN THE SENATE OF THE UNITED STATES

MAY 18 (legislative day, MAY 16), 1977

Mr. KENNEDY (for himself, Mr. BAYH, Mr. EASTLAND, Mr. INOUYE, Mr. MCCLELLAN, Mr. MATHIAS, Mr. NELSON, Mr. THURMOND, Mr. HUDDLESTON, and Mr. GARN) introduced the following bill; which was read twice and referred by unanimous consent to the Committee on the Judiciary, and, if and when reported, then to the Select Committee on Intelligence

NOVEMBER 15 (legislative day, NOVEMBER 1), 1977

Reported by Mr. KENNEDY, with amendments

[Omit the part struck through and insert the part printed in italic]

NOVEMBER 15 (legislative day, NOVEMBER 1), 1977

Referred, by unanimous consent, to the Select Committee on Intelligence

MARCH 14 (legislative day, FEBRUARY 6), 1978

Reported by Mr. BAYH, with amendments

[Omit the part in boldface brackets and insert the part in boldface italic]

A BILL

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*
3 That this Act may be cited as the "Foreign Intelligence
4 Surveillance Act of 1977" **[***1978***]**.

5 SEC. 2. Title 18, United States Code, is amended by
6 adding a new chapter after chapter 119 as follows:

II

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 **"Chapter 120.—ELECTRONIC SURVEILLANCE WITH-**
2 **IN THE UNITED STATES FOR FOREIGN INTEL-**
3 **LIGENCE PURPOSES**

"Sec.
"2521. Definitions.
"2522. Authorization for electronic surveillance for foreign intelligence purposes.
"2523. Designation of judges authorized to grant orders for electronic surveillance.
"2524. Application for an order.
"2525. Issuance of an order.
"2526. Use of information.
"2527. Report of electronic surveillance."
"2528. Congressional oversight.

4 **"§ 2521. Definitions**

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

8 "(b) As used in this chapter—

9 "(1) 'Foreign power' means—

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

13 "(B) a faction of a foreign nation or nations,
14 not substantially composed of United States
15 persons;

16 "(C) an entity, which is openly acknowledged
17 by a foreign government or governments to be
18 directed and controlled by such foreign government
19 or governments;

20 "(D) a foreign-based terrorist group;

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

"(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—~~

[~~"(ii) 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 aids or abets a~~ *any* ~~person,~~ *knowing that such person is engaged in activities* ~~described in paragraph (ii) above;~~]

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

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

"(ii) acts for or on behalf of a foreign power which engages in clandestine intelligence

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

activities contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or conspires with any person knowing that such person is engaged in such activities;

[~~"(B) any person who—~~

[~~"(i) knowingly engages in clandestine intelligence 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~~

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

~~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) or (iii) above.~~]

"(B) any person who—

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

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

"(iii) knowingly engages in sabotage or terrorism, or activities which are or may be in

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 *preparation therefor, for or on behalf of a*
2 *foreign power;*
3 *"(iv) knowingly aids or abets any person*
4 *in the conduct of activities described in sub-*
5 *paragraph (B) (i) through (iii) above, or*
6 *conspires with any person knowing that such*
7 *person is engaged in activities described in*
8 *subparagraph (B) (i) through (iii) above:*
9 *Provided, That no United States person may*
10 *be considered an agent of a foreign power solely*
11 *upon the basis of activities protected by the first*
12 *amendment to the Constitution of the United*
13 *States.*
14 "(3) 'Terrorism' means activities which—
15 "(A) are violent acts or acts dangerous to
16 human life which would be criminal under the laws
17 of the United States or of any State if committed
18 within its jurisdiction; and
19 "(B) appear to be intended—
20 "(i) to intimidate or coerce the civilian
21 population,
22 "(ii) to influence the policy of a govern-
23 ment by intimidation or coercion, or
24 "(iii) to affect the conduct of a govern-
25 ment by assassination or kidnaping.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(4) 'Sabotage' means activities which would be
2 prohibited by title 18, United States Code, chapter 105,
3 if committed against the United States.
4 "(5) 'Foreign intelligence information' means—
5 [~~"(A) information which relates to, and is~~
6 ~~deemed necessary to the ability of the United~~
7 ~~States to protect itself against, actual or potential~~
8 ~~attack or other grave hostile acts of a foreign power~~
9 ~~or an agent of a foreign power;~~
10 [~~"(B) information with respect to a foreign~~
11 ~~power or foreign territory, which relates to, and~~
12 ~~because of its importance is deemed essential to—~~
13 [~~"(i) the national defense or the security~~
14 ~~of the Nation; or~~
15 [~~"(ii) the successful conduct of the foreign~~
16 ~~affairs of the United States;~~
17 [~~"(C) information which relates to, and is~~
18 ~~deemed necessary to the ability of the United States~~
19 ~~to protect against terrorism by a foreign power or an~~
20 ~~agent of a foreign power;~~
21 [~~"(D) information which relates to, and is~~
22 ~~deemed necessary to the ability of the United States~~
23 ~~to protect against sabotage by a foreign power or an~~
24 ~~agent of a foreign power; or~~
25 [~~"(E) information which relates to, and is~~

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 ~~deemed necessary to the ability of the United States~~
2 ~~to protect against the clandestine intelligence activi-~~
3 ~~ties of an intelligence service or network of a foreign~~
4 ~~power or an agent of a foreign power.~~]
5 *"(A) information which relates to, and if con-*
6 *cerning a United States person is necessary to, the*
7 *ability of the United States to protect itself against*
8 *actual or potential attack or other grave hostile acts*
9 *of a foreign power or an agent of a foreign power;*
10 *"(B) information with respect to a foreign*
11 *power or foreign territory which relates to, and if*
12 *concerning a United States person is necessary to—*
13 *"(i) the national defense or the security*
14 *of the Nation; or*
15 *"(ii) the successful conduct of the foreign*
16 *affairs of the United States; or*
17 *"(C) information which relates to, and if con-*
18 *cerning a United States person is necessary to, the*
19 *ability of the United States to protect against—*
20 *"(i) sabotage or terrorism by a foreign*
21 *power or an agent of a foreign power, or*
22 *"(ii) the clandestine intelligence activities*
23 *of an intelligence service or network of a foreign*
24 *power or an agent of a foreign power.*
25 "(6) 'Electronic surveillance' means—

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(A) the acquisition by an electronic, mechan-
2 ical, or other surveillance device of the contents of
3 any wire or radio communication sent by or intended
4 to be received by a particular, known United States
5 person who is in the United States, where the con-
6 tents are acquired by intentionally targeting that
7 United States person, under circumstances in which
8 a person has a reasonable expectation of privacy and
9 a warrant would be required for law enforcement
10 purposes;
11 "(B) the acquisition by an electronic, mechan-
12 ical, or other surveillance device, of the contents of
13 any wire communication to or from a person in the
14 United States, without the consent of any party
15 thereto, where such acquisition occurs in the United
16 States while the communication is being trans-
17 mitted by wire;
18 "(C) the intentional acquisition, by an elec-
19 tronic, mechanical, or other surveillance device, of
20 the contents of any radio communication, under
21 circumstances in which a person has a reasonable
22 expectation of privacy and a warrant would be
23 required for law enforcement purposes, and where
24 both the sender and all intended recipients are lo-
25 cated within the United States; or

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(D) the installation or use of an electronic,
2 mechanical, or other surveillance device in the
3 United States for monitoring to acquire information,
4 other than from a wire or radio communication,
5 under circumstances in which a person has a reason-
6 able expectation of privacy and a warrant would be
7 required for law enforcement purposes.

8 "(7) 'Attorney General' means the Attorney Gen-
9 eral of the United States (or Acting Attorney General)
10 ~~or an Assistant Attorney General specially designated~~
11 ~~in writing by the Attorney General,~~ *or the Deputy*
12 *Attorney General.*

13 "(8) 'Minimization procedures' means procedures
14 which are reasonably designed to minimize the acquisi-
15 tion ***and*** retention, and *prohibit the* dissemination, *ex-*
16 *cept as provided for in subsections 2526 (a) and (b)*, of
17 any information concerning United States persons with-
18 out their consent that does not relate to the ability of
19 the United States—

20 "(A) to protect itself against actual or poten-
21 tial attack or other grave hostile acts of a foreign
22 power or an agent of a foreign power;

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

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(C) to provide for the conduct of the foreign
2 affairs of the United States;
3 "(D) to protect against terrorism by a foreign
4 power or an agent of a foreign power;
5 "(E) to protect against sabotage by a foreign
6 power or an agent of a foreign power; or
7 "(F) to protect against the clandestine in-
8 telligence activities of an intelligence service or net-
9 work of a foreign power or an agent of a foreign
10 power;
11 [~~and which are reasonably designed to insure that infor-~~
12 ~~mation which relates solely to the conduct of foreign~~
13 ~~affairs shall not be maintained in such a manner as to~~
14 ~~permit the retrieval of such information by reference to a~~
15 ~~United States person, without his consent, who was a~~
16 ~~party to a communication acquired pursuant to this~~
17 ~~chapter; and if the target of the electronic surveillance~~
18 ~~is a foreign power which qualifies as such solely on the~~
19 ~~basis that it is an entity controlled and directed by a~~
20 ~~foreign government or governments, and unless there is~~
21 ~~probable cause to believe that a substantial number of~~
22 ~~the officers or executives of such entity are officers or~~
23 ~~employees of a foreign government, or agents of a foreign~~
24 ~~power as defined in section 2521(b)(2)(B), proce-~~

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

~~dures 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.~~]

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

"(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

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 is incorporated in the United States, but not including
2 corporations *or associations* which are foreign powers
3 ***as defined in section 2521(b)(1) (A) through (E).***
4 "(10) 'United States' when used in a geographic
5 sense means all areas under the territorial sovereignty of
6 the United States, the Trust Territory of the Pacific
7 Islands, and the Canal Zone.

8 **"§ 2522. Authorization for electronic surveillance for for-**
9 **eign intelligence purposes**

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

19 **"§ 2523. Designation of judges authorized to grant orders**
20 **for electronic surveillance**

21 "(a) The Chief Justice of the United States shall pub-
22 licly designate seven district court judges ***who shall consti-***
23 ***tute a special court, each member of which*** shall have
24 jurisdiction to hear applications for and grant orders approv-
25 ing electronic surveillance anywhere within the United

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 States under the procedures set forth in this chapter, except
2 that no judge designated under this subsection shall have
3 jurisdiction of the same application for electronic surveillance
4 under this chapter which has been denied previously by
5 another judge designated under this subsection. If any judge
6 so designated denies an application for an order authorizing
7 electronic surveillance under this chapter, such judge shall
8 provide immediately for the record a written statement of
9 each reason for his decision and, on motion of the United
10 States, the record shall be transmitted, under seal, to the
11 special court of review established in subsection (b).

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

24 "(c) Proceedings under this chapter shall be conducted
25 as expeditiously as possible. The record of proceedings under

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 this chapter, including applications made and orders granted,
2 shall be sealed and maintained under security measures estab-
3 lished by the Chief Justice in consultation with the Attorney
4 General and the Director of Central Intelligence.

5 *"(d) Each judge designated under this section shall so*
6 *serve for a maximum of seven years and shall not be eligible*
7 *for redesignation: Provided, That the judges first designated*
8 *under subsection (a) shall be designated for terms of from*
9 *one to seven years so that one term expires each year, and*
10 *that judges first designated under subsection (b) shall be*
11 *designated for terms of three, five, and seven years.*

12 **"§ 2524. Application for an order**

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

21 "(1) the identity of the Federal officer making the
22 application;

23 "(2) the authority conferred on the Attorney Gen-
24 eral by the President of the United States and the ap-
25 proval of the Attorney General to make the application;

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(3) the identity or a description of the target of
2 the electronic surveillance;
3 "(4) a statement of the facts and circumstances
4 relied upon by the applicant to justify his belief that—
5 "(A) the target of the electronic surveillance
6 is a foreign power or an agent of a foreign power;
7 and
8 "(B) the facilities or the place at which the
9 electronic surveillance is directed are being used,
10 or are about to be used, by a foreign power or an
11 agent of a foreign power;
12 "(5) a statement of the proposed minimization
13 procedures;
14 "(6) when the target of the surveillance is not a
15 foreign power as defined in section 2521 (b) (1) (A),
16 (B), or (C), a detailed description of the nature of the
17 information sought;
18 "(7) a certification or certifications by the Assist-
19 ant to the President for National Security Affairs or an
20 executive branch official or officials designated by the
21 President from among those executive officers employed
22 in the area of national security or defense and appointed
23 by the President with the advice and consent of the
24 Senate—

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 [~~"(A) that the information sought is foreign~~
2 ~~intelligence information;~~]
3 *"(A) that the certifying official deems the*
4 *information sought to be foreign intelligence infor-*
5 *mation;*
6 "(B) that the purpose of the surveillance is to
7 obtain foreign intelligence information;
8 "(C) that such information cannot reasonably
9 be obtained by normal investigative techniques;
10 "(D) including a designation of the type of
11 foreign intelligence information being sought ac-
12 cording to the categories described in section 2521
13 (b) (5);
14 "(E) when the target of the surveillance is not
15 a foreign power, as defined in section 2521 (b) (1)
16 (A), (B), or (C), including a statement of the
17 basis for the certification that—
18 "(i) the information sought is the type of
19 foreign intelligence information designated; and
20 "(ii) such information cannot reasonably
21 be obtained by normal investigative techniques;
22 "(F) when the target of the surveillance is a
23 foreign power, as defined in section 2521 (b) (1)

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 (A), (B), or (C), stating the period of time for
2 which the surveillance is required to be maintained;
3 "(8) when the target of the surveillance is not a
4 foreign power, as defined in section 2521 (b) (1) (A)
5 (B), or (C), a statement of the means by which the
6 surveillance will be effected, and when the target is a
7 foreign power, as defined in section 2521 (b) (1) (A),
8 (B), or (C), a designation of the type of electronic sur-
9 veillance to be used according to the categories described
10 in section 2521 (b) (6), *and a statement whether physi-*
11 *cal entry is required to effect the surveillance;*
12 "(9) a statement of the facts concerning all previous
13 applications that have been made to any judge under
14 this chapter involving any of the persons, facilities, or
15 places specified in the application, and the action taken
16 on each previous application; and
17 "(10) when the target of the surveillance is not a
18 foreign power, as defined in section 2521 (b) (1) (A),
19 (B), or (C), a statement of the period of time for which
20 the electronic surveillance is required to be maintained.
21 If the nature of the intelligence gathering is such that
22 the approval of the use of electronic surveillance under
23 this chapter should not automatically terminate when
24 the described type of information has first been obtained,
25 a description of facts supporting the belief that addi-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 tional information of the same type will be obtained
2 thereafter.
3 "(b) The Attorney General may require any other
4 affidavit or certification from any other officer in connection
5 with the application.
6 "(c) The judge may require the applicant to furnish
7 such other information as may be necessary to make the
8 determinations required by section 2525 of this chapter.
9 **"§ 2525. Issuance of an order**
10 "(a) Upon an application made pursuant to section
11 2524 of this title, the judge shall enter an ex parte order as
12 requested or as modified approving the electronic surveil-
13 lance if he finds that—
14 "(1) the President has authorized the Attorney
15 General to approve applications for electronic surveil-
16 lance for foreign intelligence information;
17 "(2) the application has been made by a Federal
18 officer and approved by the Attorney General;
19 "(3) on the basis of the facts submitted by the
20 applicant there is probable cause to believe that—
21 "(A) the target of the electronic surveillance
22 is a foreign power or an agent of a foreign power;
23 and
24 "(B) the facilities or place at which the elec-
25 tronic surveillance is directed are being used, or are

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

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) ***and any other information furnished under section 2524(c).***

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

"(1) specify—

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

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

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

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 *(C), the designation of the type of foreign intelli-*
2 *gence information under section 2521(b)(5) sought*
3 *to be acquired*;
4 "(D) when the target of the surveillance is not
5 a foreign power, as defined in section 2521 (b) (1)
6 (A), (B), or (C), the means by which the elec-
7 tronic surveillance will be effected, and when the
8 target is a foreign power, as defined in section 2521
9 (b) (1) (A), (B), or (C), a designation of the
10 type of electronic surveillance to be used according
11 to the categories described in section 2521 (b) (6)
12 *and whether physical entry will be used to effect the*
13 *surveillance*; and
14 "(E) the period of time during which the
15 electronic surveillance is approved; and
16 "(2) direct—
17 "(A) that the minimization procedures be
18 followed;
19 "(B) that, upon the request of the applicant, a
20 specified communication or other common carrier,
21 landlord, custodian, contractor, or other specified
22 person furnish the applicant forthwith any and all
23 information, facilities, or technical assistance, neces-
24 sary to accomplish the electronic surveillance in such
25 manner as will protect its secrecy and produce a

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 minimum of interference with the services that such
2 carrier, landlord, custodian, contractor, or other per-
3 son is providing that target of electronic surveillance;
4 "(C) that such carrier, landlord, custodian, or
5 other person maintain under security procedures
6 approved by the Attorney General and the Director
7 of Central Intelligence any records concerning the
8 surveillance or the aid furnished which such person
9 wishes to retain;
10 "(D) that the applicant compensate, at the
11 prevailing rate, such carrier, landlord, custodian, or
12 other person for furnishing such aid.
13 "(c) An order issued under this section may approve
14 an electronic surveillance not targeted against a foreign
15 power, as defined in section 2521(b)(1) (A), (B), or
16 (C), for the period necessary to achieve its purpose, or for
17 ninety days, whichever is less; an order under this section
18 shall approve an electronic surveillance targeted against a
19 foreign power, as defined in section 2521(b)(1) (A),
20 (B), or (C), for the period specified in the certification
21 required in section 2524(a)(7)(F), or for one year, which-
22 ever is less. Extensions of an order issued under this chapter
23 may be granted on the same basis as an original order upon
24 an application for an extension made in the same manner as
25 required for an original application and after new findings

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 required by subsection (a) of this section. In connection
2 with applications for extensions where the target is not a for-
3 eign power, as defined in section 2521 (b) (1) (A), (B), or
4 (C), the judge may require the applicant to submit informa-
5 tion, obtained pursuant to the original order or to any previ-
6 ous extensions, as may be necessary to make new findings of
7 probable cause. ***At the end of the period of time for which***
8 ***an electronic surveillance is approved by an order or an***
9 ***extension issued under this section, the judge may assess***
10 ***compliance with the minimization procedures required by***
11 ***this chapter.***
12 "(d) Notwithstanding any other provision of this
13 chapter when the Attorney General reasonably determines
14 that—
15 "(1) an emergency situation exists with respect to
16 the employment of electronic surveillance to obtain for-
17 eign intelligence information before an order authorizing
18 such surveillance can with due diligence be obtained, and
19 "(2) the factual basis for issuance of an order under
20 this chapter to approve such surveillance exists, he may
21 authorize the emergency employment of electronic sur-
22 veillance if a judge designated pursuant to section 2523
23 of this chapter is informed by the Attorney General or
24 his designate at the time of such authorization that the
25 decision has been made to employ emergency electronic

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 surveillance and if an application in accordance with this
2 chapter is made to that judge as soon as practicable, but
3 not more than twenty-four hours after the Attorney Gen-
4 eral authorizes such acquisition. If the Attorney General
5 authorizes such emergency employment of electronic
6 surveillance, he shall require that the minimization proce-
7 dures required by this chapter for the issuance of a judi-
8 cial order be followed. In the absence of a judicial order
9 approving such electronic surveillance, the surveillance
10 shall terminate when the information sought is obtained,
11 when the application for the order is denied, or after the
12 expiration of twenty-four hours from the time of au-
13 thorization by the Attorney General, whichever is earli-
14 est. In the event that such application for approval is
15 denied, or in any other case where the electronic sur-
16 veillance is terminated without an order having been
17 issued, no information obtained or evidence derived from
18 such surveillance shall be received in evidence or other-
19 wise disclosed in any trial, hearing, or other proceeding
20 in or before any court, grand jury, department, office,
21 agency, regulatory body, legislative committee, or other
22 authority of the United States, a State, or political sub-
23 division thereof; ***and no information concerning any***
24 ***United States person acquired from such surveillance***
25 ***shall subsequently be used or disclosed in any other***

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 *manner by Federal officers or employees without the*
2 *consent of such person, except with the approval of the*
3 *Attorney General where the information indicates a*
4 *threat of death or serious bodily harm to any person.*
5 A denial of the application made under this subsection
6 may be reviewed as provided in section 2523.

7 **"§ 2526. Use of information**

8 "(a) Information concerning United States persons
9 acquired from an electronic surveillance conducted pursuant
10 to this chapter may be used and disclosed by Federal officers
11 and employees without the consent of the United States per-
12 son only for purposes specified in section 2521 (b) (8) (A)
13 through (F) *and in accordance with the minimization pro-*
14 *cedures required by this chapter,* or for the enforcement of
15 the criminal law if its use outweighs the possible harm to
16 the national security. No otherwise privileged communica-
17 tion obtained in accordance with, or in violation of, the
18 provisions of this chapter shall lose its privileged character.
19 *No information acquired from an electronic surveillance*
20 *conducted pursuant to this chapter may be used or disclosed*
21 *by Federal officers or employees except for lawful purposes.*
22 "(b) The minimization procedures required under this
23 chapter shall not preclude the retention and disclosure, for
24 law enforcement purposes, of any information which consti-
25 tutes evidence of a crime if such disclosure is accompanied

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 by a statement that such evidence, or any information de-
2 rived therefrom, may only be used in a criminal proceeding
3 with the advance authorization of the Attorney General.
4 "(c) Whenever the Government ***of the United States,***
5 ***of a State, or of a political subdivision thereof*** intends to
6 enter into evidence or otherwise use or disclose in any trial,
7 hearing, or other proceeding in or before any court, depart-
8 ment, officer, agency, or other authority of the United
9 States, *a State, or a political subdivision thereof,* any infor-
10 mation obtained or derived from an electronic surveillance,
11 the Government shall prior to the trial, hearing, or other
12 proceeding or at a reasonable time prior to an effort to so
13 disclose or so use the information or submit it in evidence
14 notify the court in which the information is to be disclosed or
15 used or, if the information is to be disclosed or used in or
16 before another authority, shall notify a court in the district
17 wherein the information is to be so disclosed or so used that
18 the Government intends to so disclose or so use such infor-
19 mation. ~~Whenever any court is so notified, or whenever a~~
20 ~~motion is made pursuant to section 3504 of this title, or any~~
21 ~~other statute or rule of the United States to suppress evidence~~
22 ~~on the grounds that it was obtained or derived from an un-~~
23 ~~lawful electronic surveillance, the court, or where the mo-~~
24 ~~tion is made before another authority, a court in the same~~
25 ~~district as the authority, shall notwithstanding any other~~

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 ~~law, if the Government by affidavit asserts that an adversary~~
2 ~~hearing would harm the national security or the foreign~~
3 ~~affairs of the United States, review in camera and ex parte~~
4 ~~the application, order, and so much of the transcript of the~~
5 ~~surveillance as may be necessary to determine whether the~~
6 ~~surveillance was authorized and conducted in a manner that~~
7 ~~did not violate any right afforded by the Constitution and~~
8 ~~statutes of the United States to the person aggrieved: *Pro-*~~
9 ~~*vided,* That in making this determination, the court shall dis-~~
10 ~~close to the aggrieved person portions of the application,~~
11 ~~order, or transcript only where such disclosure is necessary~~
12 ~~for an accurate determination of the legality of the surveil-~~
13 ~~lance. If the court determines that the electronic surveillance~~
14 ~~of the person aggrieved was not lawfully authorized or con-~~
15 ~~ducted, the court shall in accordance with the requirements~~
16 ~~of law suppress that information which was obtained or~~
17 ~~evidence derived unlawfully from the electronic surveillance~~
18 ~~of the person aggrieved.~~
19 *"(d) Any person who has been a subject of electronic*
20 *surveillance and against whom evidence derived from such*
21 *electronic surveillance is to be, or has been, introduced or*
22 *otherwise used or disclosed in any trial, hearing, or proceeding*
23 *in or before any court, department officer, agency, regulatory*
24 *body, or other authority of the United States, a State, or a*

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 *political subdivision thereof, may move to suppress the con-*
2 *tents of any communication acquired by electronic surveil-*
3 *lance, or evidence derived therefrom, on the grounds that—*
4 *"(1) the communication was unlawfully acquired;*
5 *or*
6 *"(2) the surveillance was not made in conformity*
7 *with the order of authorization or approval.*
8 *Such motion shall be made before the trial, hearing, or pro-*
9 *ceeding unless there was no opportunity to make such motion*
10 *or the person was not aware of the grounds of the motion.*
11 *"(e) Whenever any court is notified in accordance with*
12 *subsection (c), or whenever a motion is made by an aggrieved*
13 *person pursuant to subsection (d), to suppress evidence on*
14 *the grounds that it was obtained or derived from an unlawful*
15 *electronic surveillance, or whenever any motion or request is*
16 *made by an aggrieved person pursuant to section 3504 of this*
17 *title or any other statute or rule of the United States, to dis-*
18 *cover, obtain, or suppress evidence or information obtained or*
19 *derived from electronic surveillance, the Federal court, or*
20 *where the motion is made before another authority, a Federal*
21 *court in the same district as the authority, shall, notwithstand-*
22 *ing any other law, if the Govrnment by affidavit asserts that*
23 *disclosure or an adversary hearing would harm the national*
24 *security of the United States, review in camera and ex parte*
25 *the application, order, and other materials relating to the sur-*

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 *veillance as may be necessary to determine whether the surveil-*
2 *lance was authorized and conducted in a manner that did not*
3 *violate any right afforded by the Constitution and statutes of*
4 *the United States to the aggrieved person. In making this*
5 *determination, the court shall disclose to the aggrieved person*
6 *portions of the application, order, or other materials relating*
7 *to the survillance only where such disclosure is necessary to*
8 *make an accurate determination of the legality of the surveil-*
9 *lance. If the court determines that the electronic surveillance*
10 *of the aggrieved person was not lawfully authorized or*
11 *conducted, the court shall in accordance with the requirements*
12 *of law suppress the information obtained or evidence derived*
13 *from the unlawful electronic surveillance. If the court deter-*
14 *mines that the surveillance was lawfully authorized and con-*
15 *ducted, the court shall deny any motion for disclosure or*
16 *discovery unless required by due process.*

17 "~~(d)~~ *(f)* If an emergency employment of the electronic
18 surveillance is authorized under section 2525 (d) and a sub-
19 sequent order approving the surveillance is not obtained, the
20 judge shall cause to be served on any United States person
21 named in the application and on such other United States
22 persons subject to electronic surveillance as the judge may
23 determine in his discretion it is in the interest of justice to
24 serve, notice of—

25 "(1) the fact of the application;

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(2) the period of the surveillance; and

2 "(3) the fact that during the period information

3 was or was not obtained.

4 On an ex parte showing of good cause to the judge the serv-

5 ing of the notice required by this subsection may be post-

6 poned or suspended for a period not to exceed ninety days.

7 Thereafter, on a further ex parte showing of good cause, the

8 court shall forego ordering the serving of the notice required

9 under this subsection.

10 *"(g) In circumstances involving the unintentional*

11 *acquisition, by an electronic, mechanical, or other surveil-*

12 *lance device of the contents of any radio communication,*

13 *under circumstances in which a person has a reasonable*

14 *expectation of privacy and a warrant would be required*

15 *for law enforcement purposes, and where both the sender*

16 *and all intended recipients are located within the United*

17 *States, such contents shall be destroyed upon recognition,*

18 *except with the approval of the Attorney General where the*

19 *contents indicate a threat of death or serious bodily harm*

20 *to any person.*

21 **"§ 2527. Report of electronic surveillance**

22 "In April of each year, the Attorney General shall

23 report to the Administrative Office of the United States

24 Courts and shall transmit to Congress with respect to the

25 preceding calendar year—

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(1) the total number of applications made for
2 orders and extensions of orders approving electronic
3 surveillance; and
4 "(2) the total number of such orders and exten-
5 sions either granted, modified, or denied.
6 "§ *2528. Congressional oversight*
7 *"(a) On a semiannual basis the Attorney General shall*
8 *fully inform the House Permanent Select Committee on In-*
9 *telligence and the Senate Select Committee on Intelligence*
10 *concerning all electronic surveillance under this chapter.*
11 *Nothing in this chapter shall be deemed to limit the author-*
12 *ity and responsibility of those committees to obtain such*
13 *additional information as they may need to carry out their*
14 *respective functions and duties.*
15 *"(b) On or before one year after the effective date of*
16 *this chapter, and on the same day each year thereafter, the*
17 *Select Committee on Intelligence of the United States Senate*
18 *shall report to the Senate, concerning the implementation of*
19 *this chapter. Said reports shall include but not be limited*
20 *to an analysis and recommendations concerning whether*
21 *this chapter should be (1) amended, (2) repealed, or (3)*
22 *permitted to continue in effect without amendment.*
23 *"(c) In the event the Select Committee on Intelligence*
24 *of the United States Senate shall report that this chapter*
25 *should be amended or repealed, it shall report out legislation*

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 *embodying its recommendations within thirty calendar days,*
2 *unless the Senate shall otherwise determine by yeas and nays.*
3 *"(d) Any legislation so reported shall become the pend-*
4 *ing business of the Senate with time for debate equally*
5 *divided between the proponents and opponents and shall be*
6 *voted on within thirty calendar days thereafter, unless the*
7 *Senate shall otherwise determine by years and nays.*
8 *"(e) Such legislation passed by the Senate shall be*
9 *referred to the appropriate committee of the other House*
10 *and shall be reported out by such committee together with*
11 *its recommendations within thirty calendar days and shall*
12 *thereupon become the pending business of such House and*
13 *shall be voted upon within three calendar days, unless such*
14 *House shall otherwise determine by yeas and nays.*
15 *"(f) In the case of any disagreement between the two*
16 *Houses of Congress with respect to such legislation passed*
17 *by both Houses, conferees shall be promptly appointed and*
18 *the committee of conference shall make and file a report with*
19 *respect to such legislation within seven calendar days after*
20 *the legislation is referred to the committee of conference.*
21 *Notwithstanding any rule in either House concerning the*
22 *printing of conference reports in the record or concerning*
23 *any delay in the consideration of such reports, such reports*
24 *shall be acted on by both Houses not later than seven*

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 *calendar days after the conference report is filed. In the*
2 *event the conferees are unable to agree within three cal-*
3 *endar days they shall report to their respective Houses in*
4 *disagreement.*".

5 SEC. 3. The provisions of this Act and the amendment
6 made hereby shall become effective upon enactment: *Pro-*
7 *vided,* That any electronic surveillance approved by the
8 Attorney General to gather foreign intelligence information
9 shall not be deemed unlawful for failure to follow the proce-
10 dures of chapter 120, title 18, United States Code, if that sur-
11 veillance is terminated or an order approving that surveillance
12 is obtained under this chapter within ninety days following
13 the designation of the first judge pursuant to section 2523 of
14 chapter 120, title 18, United States Code.

15 SEC. 4. Chapter 119 of title 18, United States Code, is
16 amended as follows:

17 (a) Section 2511 (1) is amended—

18 (1) by inserting "or chapter 120 or with respect to
19 techniques used by law enforcement officers not involv-
20 ing the interception of wire or oral communications
21 as otherwise authorized by a search warrant or order of
22 a court of competent jurisdiction," immediately after
23 "chapter" in the first sentence;

24 (2) by inserting a comma and "or, under color of

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 law, willfully engages in any other form of electronic
2 surveillance as defined in chapter 120" immediately
3 before the semicolon in paragraph (a);
4 (3) by inserting "or information obtained under
5 color of law by any other form of electronic surveillance
6 as defined in chapter 120" immediately after "contents
7 of any wire or oral communication" in paragraph (c);
8 (4) by inserting "or any other form of electronic
9 surveillance, as defined in chapter 120," immediately
10 before "in violation" in paragraph (c);
11 "(5) by inserting "or information obtained under
12 color of law by any other form of electronic surveillance
13 as defined in chapter 120" immediately after "any wire
14 or oral communication" in paragraph (d); and
15 (6) by inserting "or any other form of electronic
16 surveillance, as defined in chapter 120," immediately
17 before "in violation" in paragraph (d).
18 (b) (1) Section 2511 (2) (a) (i) is amended by insert-
19 ing the words "or radio communication" after the words
20 "wire communication" and by inserting the words "or other-
21 wise acquire" after the word "intercept".
22 (2) Section 2511 (2) (a) (ii) is amended by inserting
23 the words "or chapter 120" after the second appearance of
24 the word "chapter," and by striking the period at the end

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 thereof and adding the following: "or engage in electronic
2 surveillance, as defined in chapter 120: *Provided, however,*
3 That before the information, facilities, or technical assistance
4 may be provided, the investigative or law enforcement officer
5 shall furnish to the officer, employee, or agent of the carrier
6 either—

7 "(1) an order signed by the authorizing judge certi-
8 fying that a court order directing such assistance has
9 been issued; or

10 "(2) in the case of an emergency interception or
11 electronic surveillance as provided for in section 2518
12 (7) of this chapter or section 2525 (d) of chapter 120,
13 a certification under oath by the investigative or law
14 enforcement officer that the applicable statutory require-
15 ments have been met,

16 and setting forth the period of time for which the electronic
17 surveillance is authorized and describing the facilities from
18 which the communication is to be acquired. Any violation of
19 this subsection by a communication common carrier or an
20 officer, employee, or agency thereof, shall render the carrier
21 liable for the civil damages provided for in section 2520. ***No***
22 ***communication common carrier or officer, employee, or***
23 ***agent thereof shall disclose the existence of any interception***
24 ***under this chapter or electronic surveillance, as defined in***

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 ***chapter 120, with respect to which the common carrier***
2 ***has been furnished either an order or certification under***
3 ***this subparagraph, except as may otherwise be lawfully***
4 ***ordered.".***

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

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

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

15 "(e) Notwithstanding any other provision of this title
16 or sections 605 or 606 of the Communications Act of 1934,
17 it shall not be unlawful for an officer, employee, or agent of
18 the United States in the normal course of his official duty
19 ***under procedures approved by the Attorney General*** to
20 conduct electronic surveillance as defined in section 2521
21 (b) (6) of chapter 120 without a court order for the sole
22 purpose of:

23 "(i) testing the capability of electronic equipment,
24 provided that *no particular United States person shall*
25 *be intentionally targeted for testing purposes without*

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 *his consent,* the test period shall be limited in extent
2 and duration to that necessary to determine the capabil-
3 ity of the equipment, that the content of any communica-
4 tion acquired under this paragraph shall be retained
5 and used only for the purpose of determining the ca-
6 pability of such equipment, shall be disclosed only to the
7 persons conducting the test, and shall be destroyed upon
8 completion of the testing, and that the test may exceed
9 ninety days only with the prior approval of the Attorney
10 General; or
11 "(ii) determining the existence and capability of
12 electronic surveillance equipment being used unlawfully,
13 provided ***that no particular United States person shall***
14 ***be intentionally targeted for such purposes without his***
15 ***consent,*** that such electronic surveillance shall be limited
16 in extent and duration to that necessary to determine
17 the existence and capability of such equipment, and that
18 any information acquired by such surveillance shall be
19 used only to enforce this chapter or section 605 of the
20 Communications Act of 1934 or to protect information
21 from unlawful electronic surveillance.
22 "(f) Nothing contained in this chapter, or section 605
23 of the Communications Act of 1934 (47 U.S.C. 605) shall
24 be deemed to affect the acquisition by the United States
25 Government of foreign intelligence information from inter-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 national *or foreign* communications by a means other than
2 electronic surveillance as defined in section 2521 (b) (6)
3 of this title; and the procedures in this chapter and chapter
4 120 of this title, shall be the exclusive means by which
5 electronic surveillance, as defined in section 2521 (b) (6)
6 of chapter 120, and the interception of domestic wire and
7 oral communications may be conducted.".

8 (d) Section 2511 (3) is repealed.

9 (e) Section 2515 is amended by inserting the words
10 "or electronic surveillance, as defined in chapter 120, has
11 been conducted" after the word "intercepted", by inserting
12 the words "or other information obtained from electronic
13 surveillance, as defined in chapter 120," after the second
14 appearance of the word "communication", and by inserting
15 "or chapter 120" after the final appearance of the word
16 "chapter".

17 (f) Section 2518 (1) is amended by inserting the words
18 "under this chapter" after the word "communication".

19 (g) Section 2518 (4) is amended by inserting the
20 words "under this chapter" after both appearances of the
21 words "wire or oral communication".

22 (h) Section 2518 (9) is amended by striking the word
23 "intercepted" and inserting the words "intercepted pursuant
24 to this chapter" after the word "communication".

25 *(i) Section 2518(10) is amended by striking the word*

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 *"intercepted" and inserting the words "intercepted pursuant*
2 *to this chapter" after the first appearance of the word "com-*
3 *munication".*

4 ~~(i)~~ *(j)* Section 2519 (3) is amended by inserting the
5 words "pursuant to this chapter" after the words "wire or
6 oral communications" and after the words "granted or de-
7 nied".

8 ~~(j)~~ *(k)* Section 2520 is amended by deleting all below
9 subsection (2) and inserting in lieu thereof: "Any person
10 other than a foreign power or an agent of a foreign power
11 as defined in sections 2521 (b) (1) and 2521 (b) (2) (A)
12 of chapter 120, who has been subject to electronic surveil-
13 lance, as defined in chapter 120, or whose wire or oral com-
14 munciation has been intercepted, or about whom information
15 has been disclosed or used, in violation of this chapter, shall
16 (1) have a civil cause of action against any person who so
17 acted in violation of this chapter and".

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Calendar No. 643

95TH CONGRESS
2D SESSION

S. 1566

[Report No. 95–604]
[Report No. 95–701]

A BILL

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.

By Mr. KENNEDY, Mr. BAYH, Mr. EASTLAND, Mr. INOUYE, Mr. MCCLELLAN, Mr. MATHIAS, Mr. NELSON, Mr. THURMOND, Mr. HUDDLESTON, and Mr. GARN

MAY 18 (legislative day, MAY 16), 1977
Read twice and referred by unanimous consent to the Committee on the Judiciary, and, if and when reported, then to the Select Committee on Intelligence

NOVEMBER 15 (legislative day, NOVEMBER 1), 1977
Reported with amendments

NOVEMBER 15 (legislative day, NOVEMBER 1), 1977
Referred, by unanimous consent, to the Select Committee on Intelligence

MARCH 14 (legislative day, FEBRUARY 6), 1978
Reported with amendments

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

FILE COPY

95TH CONGRESS
2D SESSION

S. 1566

IN THE HOUSE OF REPRESENTATIVES

APRIL 24, 1978

Referred to the Committee on the Judiciary

AN ACT

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*
3 That this Act may be cited as the "Foreign Intelligence
4 Surveillance Act of 1978".

5 SEC. 2. Title 18, United States Code, is amended by
6 adding a new chapter after chapter 119 as follows:

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 **"Chapter 120.—ELECTRONIC SURVEILLANCE WITH-**
2 **IN THE UNITED STATES FOR FOREIGN INTEL-**
3 **LIGENCE PURPOSES**

"Sec.
"2521. Definitions.
"2522. Authorization for electronic surveillance for foreign intelligence purposes.
"2523. Designation of judges authorized to grant orders for electronic surveillance.
"2524. Application for an order.
"2525. Issuance of an order.
"2526. Use of information.
"2527. Report of electronic surveillance.
"2528. Congressional oversight.

4 **"§ 2521. Definitions**

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

8 "(b) As used in this chapter—

9 "(1) 'Foreign power' means—

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

13 "(B) a faction of a foreign nation or nations,
14 not substantially composed of United States
15 persons;

16 "(C) an entity, which is openly acknowledged
17 by a foreign government or governments to be
18 directed and controlled by such foreign government
19 or governments;

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(D) a foreign-based terrorist group;
2 "(E) a foreign-based political organization, not
3 substantially composed of United States persons; or
4 "(F) an entity which is directed and controlled
5 by a foreign government or governments.
6 "(2) 'Agent of a foreign power' means—
7 "(A) any person, other than a United States
8 person, who—
9 "(i) acts in the United States as an officer
10 or employee of a foreign power; or
11 "(ii) acts for or on behalf of a foreign
12 power which engages in clandestine intelligence
13 activities contrary to the interests of the United
14 States, when the circumstances of such person's
15 presence in the United States indicate that such
16 person may engage in such activities in the
17 United States, or when such person knowingly
18 aids or abets any person in the conduct of such
19 activities or conspires with any person knowing
20 that such person is engaged in such activities;
21 "(B) any person who—
22 "(i) knowingly engages in clandestine in-
23 telligence gathering activities for or on behalf
24 of a foreign power, which activities involve or

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 may involve a violation of the criminal statutes
2 of the United States;
3 "(ii) pursuant to the direction of an intel-
4 ligence service or network of a foreign power,
5 knowingly engages in any other clandestine in-
6 telligence activities for or on behalf of such for-
7 eign power, which activities involve or are about
8 to involve a violation of the criminal statutes
9 of the United States;
10 "(iii) knowingly engages in sabotage or
11 terrorism, or activities in furtherance thereof,
12 for or on behalf of a foreign power;
13 "(iv) knowingly aids or abets any person
14 in the conduct of activities described in sub-
15 paragraph (B) (i) through (iii) above, or
16 conspires with any person knowing that such
17 person is engaged in activities described in
18 subparagraph (B) (i) through (iii) above:
19 *Provided,* That no United States person may
20 be considered an agent of a foreign power solely
21 upon the basis of activities protected by the first
22 amendment to the Constitution of the United
23 States.
24 "(3) 'Terrorism' means activities which—
25 "(A) are violent acts or acts dangerous to

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 human life which would be criminal under the laws
2 of the United States or of any State if committed
3 within its jurisdiction; and
4 "(B) appear to be intended—
5 "(i) to intimidate or coerce the civilian
6 population,
7 "(ii) to influence the policy of a govern-
8 ment by intimidation or coercion, or
9 "(iii) to affect the conduct of a govern-
10 ment by assassination or kidnaping.
11 "(4) 'Sabotage' means activities which would be
12 prohibited by title 18, United States Code, chapter 105,
13 if committed against the United States.
14 "(5) 'Foreign intelligence information' means—
15 "(A) information which relates to, and if con-
16 cerning a United States person is necessary to, the
17 ability of the United States to protect itself against
18 actual or potential attack or other grave hostile acts
19 of a foreign power or an agent of a foreign power;
20 "(B) information with respect to a foreign
21 power or foreign territory which relates to, and if
22 concerning a United States person is necessary to—
23 "(i) the national defense or the security
24 of the Nation; or

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(ii) the successful conduct of the foreign
2 affairs of the United States; or
3 "(C) information which relates to, and if con-
4 cerning a United States person is necessary to, the
5 ability of the United States to protect against—
6 "(i) sabotage or terrorism by a foreign
7 power or an agent of a foreign power, or
8 "(ii) the clandestine intelligence activities
9 of an intelligence service or network of a foreign
10 power or an agent of a foreign power.
11 "(6) 'Electronic surveillance' means—
12 "(A) the acquisition by an electronic, mechan-
13 ical, or other surveillance device of the contents of
14 any wire or radio communication sent by or intended
15 to be received by a particular, known United States
16 person who is in the United States, where the con-
17 tents are acquired by intentionally targeting that
18 United States person, under circumstances in which
19 a person has a reasonable expectation of privacy and
20 a warrant would be required for law enforcement
21 purposes;
22 "(B) the acquisition by an electronic, mechan-
23 ical, or other surveillance device, of the contents of
24 any wire communication to or from a person in the
25 United States, without the consent of any party

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 thereto, where such acquisition occurs in the United
2 States while the communication is being trans-
3 mitted by wire;
4 "(C) the intentional acquisition, by an elec-
5 tronic, mechanical, or other surveillance device, of
6 the contents of any radio communication, under
7 circumstances in which a person has a reasonable
8 expectation of privacy and a warrant would be
9 required for law enforcement purposes, and where
10 both the sender and all intended recipients are lo-
11 cated within the United States; or
12 "(D) the installation or use of an electronic,
13 mechanical, or other surveillance device in the
14 United States for monitoring to acquire information,
15 other than from a wire or radio communication,
16 under circumstances in which a person has a reason-
17 able expectation of privacy and a warrant would be
18 required for law enforcement purposes.
19 "(7) 'Attorney General' means the Attorney Gen-
20 eral of the United States (or Acting Attorney General)
21 or the Deputy Attorney General.
22 "(8) 'Minimization procedures' means procedures
23 which are reasonably designed to minimize the acquisi-
24 tion and retention, and prohibit the dissemination, ex-
25 cept as provided for in subsections 2526 (a) and (b), of

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 any information concerning United States persons with-
2 out their consent that does not relate to the ability of
3 the United States—

4 "(A) to protect itself against actual or poten-
5 tial attack or other grave hostile acts of a foreign
6 power or an agent of a foreign power;

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

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

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

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

15 "(F) to protect against the clandestine intel-
16 ligence activities of an intelligence service or net-
17 work of a foreign power or an agent of a foreign
18 power;

19 and which are reasonably designed to insure that in-
20 formation which relates solely to the ability of the
21 United States to provide for the national defense or
22 security of the Nation and to provide for the conduct
23 of foreign affairs of the United States, under subpara-
24 graphs (B) and (C) above, shall not be disseminated
25 in a manner which identifies any United States person,

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

without such person's consent, unless such person's identity is necessary to understand or assess the importance of information with respect to a foreign power or foreign territory or such information is otherwise publicly available.

"(9) 'United States person' means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence or a corporation which is incorporated in the United States, but not including corporations or associations which are foreign powers as defined in section 2521(b)(1)(A) through (E).

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

"§2522. Authorization for electronic surveillance for foreign intelligence purposes

"Applications for a court order under this chapter are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to Federal judges having jurisdiction under section 2523 of

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 this chapter, and a judge to whom an application is made
2 may grant an order, in conformity with section 2525 of this
3 chapter, approving electronic surveillance of a foreign power
4 or an agent of a foreign power for the purpose of obtaining
5 foreign intelligence information.

6 **"§ 2523. Designation of judges authorized to grant orders**
7 **for electronic surveillance**

8 "(a) The Chief Justice of the United States shall pub-
9 licly designate seven district court judges who shall consti-
10 tute a special court, each member of which shall have
11 jurisdiction to hear applications for and grant orders approv-
12 ing electronic surveillance anywhere within the United
13 States under the procedures set forth in this chapter, except
14 that no judge designated under this subsection shall have
15 jurisdiction of the same application for electronic surveillance
16 under this chapter which has been denied previously by
17 another judge designated under this subsection. If any judge
18 so designated denies an application for an order authorizing
19 electronic surveillance under this chapter, such judge shall
20 provide immediately for the record a written statement of
21 each reason for his decision and, on motion of the United
22 States, the record shall be transmitted, under seal, to the
23 special court of review established in subsection (b).

24 "(b) The Chief Justice shall publicly designate three
25 judges, one of whom shall be publicly designated as the pre-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 siding judge, from the United States district courts or courts
2 of appeals who together shall comprise a special court of
3 review which shall have jurisdiction to review the denial of
4 any application made under this chapter. If such special
5 court determines that the application was properly denied,
6 the special court shall immediately provide for the record
7 a written statement of each reason for its decision and, on
8 petition of the United States for a writ of certiorari, the
9 record shall be transmitted under seal to the Supreme Court,
10 which shall have jurisdiction to review such decision.

11 "(c) Proceedings under this chapter shall be conducted
12 as expeditiously as possible. The record of proceedings under
13 this chapter, including applications made and orders granted,
14 shall be sealed and maintained under security measures estab-
15 lished by the Chief Justice in consultation with the Attorney
16 General and the Director of Central Intelligence.

17 "(d) Each judge designated under this section shall so
18 serve for a maximum of seven years and shall not be eligible
19 for redesignation: *Provided,* That the judges first designated
20 under subsection (a) shall be designated for terms of from
21 one to seven years so that one term expires each year, and
22 that judges first designated under subsection (b) shall be
23 designated for terms of three, five, and seven years.

24 **"§ 2524. Application for an order**

25 "(a) Each application for an order approving electronic

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 surveillance under this chapter shall be made by a Federal
2 officer in writing upon oath or affirmation to a judge having
3 jurisdiction under section 2523 of this chapter. Each appli-
4 cation shall require the approval of the Attorney General
5 based upon his finding that it satisfies the criteria and require-
6 ments of such application as set forth in this chapter. It shall
7 include the following information—

8 "(1) the identity of the Federal officer making the
9 application;

10 "(2) the authority conferred on the Attorney Gen-
11 eral by the President of the United States and the ap-
12 proval of the Attorney General to make the application;

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

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

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

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

24 "(5) a statement of the proposed minimization
25 procedures;

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(6) when the target of the surveillance is not a
2 foreign power as defined in section 2521 (b) (1) (A),
3 (B), or (C), a detailed description of the nature of the
4 information sought;
5 "(7) a certification or certifications by the Assist-
6 ant to the President for National Security Affairs or an
7 executive branch official or officials designated by the
8 President from among those executive officers employed
9 in the area of national security or defense and appointed
10 by the President with the advice and consent of the
11 Senate—
12 "(A) that the certifying official deems the
13 information sought to be foreign intelligence infor-
14 mation;
15 "(B) that the purpose of the surveillance is to
16 obtain foreign intelligence information;
17 "(C) that such information cannot reasonably
18 be obtained by normal investigative techniques;
19 "(D) including a designation of the type of
20 foreign intelligence information being sought ac-
21 cording to the categories described in section 2521
22 (b) (5);
23 "(E) when the target of the surveillance is not
24 a foreign power, as defined in section 2521 (b) (1)

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 (A), (B), or (C), including a statement of the
2 basis for the certification that—
3 "(i) the information sought is the type of
4 foreign intelligence information designated; and
5 "(ii) such information cannot reasonably
6 be obtained by normal investigative techniques;
7 "(F) when the target of the surveillance is a
8 foreign power, as defined in section 2521 (b) (1)
9 (A), (B), or (C), stating the period of time for
10 which the surveillance is required to be maintained;
11 "(8) when the target of the surveillance is not a
12 foreign power, as defined in section 2521 (b) (1) (A)
13 (B), or (C), a statement of the means by which the
14 surveillance will be effected, and when the target is a
15 foreign power, as defined in section 2521 (b) (1) (A),
16 (B), or (C), a designation of the type of electronic sur-
17 veillance to be used according to the categories described
18 in section 2521 (b) (6), and a statement whether
19 physical entry is required to effect the surveillance;
20 "(9) a statement of the facts concerning all previous
21 applications that have been made to any judge under
22 this chapter involving any of the persons, facilities, or
23 places specified in the application, and the action taken
24 on each previous application; and
25 "(10) when the target of the surveillance is not a

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 foreign power, as defined in section 2521 (b) (1) (A),
2 (B), or (C), a statement of the period of time for which
3 the electronic surveillance is required to be maintained.
4 If the nature of the intelligence gathering is such that
5 the approval of the use of electronic surveillance under
6 this chapter should not automatically terminate when
7 the described type of information has first been obtained,
8 a description of facts supporting the belief that addi-
9 tional information of the same type will be obtained
10 thereafter.
11 "(b) The Attorney General may require any other
12 affidavit or certification from any other officer in connection
13 with the application.
14 "(c) The judge may require the applicant to furnish
15 such other information as may be necessary to make the
16 determinations required by section 2525 of this chapter.
17 **"§ 2525. Issuance of an order**
18 "(a) Upon an application made pursuant to section
19 2524 of this title, the judge shall enter an ex parte order as
20 requested or as modified approving the electronic surveil-
21 lance if he finds that—
22 "(1) the President has authorized the Attorney
23 General to approve applications for electronic surveil-
24 lance for foreign intelligence information;

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(2) the application has been made by a Federal
2 officer and approved by the Attorney General;
3 "(3) on the basis of the facts submitted by the
4 applicant there is probable cause to believe that—
5 "(A) the target of the electronic surveillance
6 is a foreign power or an agent of a foreign power;
7 and
8 "(B) the facilities or place at which the elec-
9 tronic surveillance is directed are being used, or are
10 about to be used, by a foreign power or an agent
11 of a foreign power;
12 "(4) the proposed minimization procedures meet
13 the definition of minimization procedures under section
14 2521 (b) (8) of this title;
15 "(5) the application which has been filed contains
16 the description and certification or certifications, spec-
17 ified in section 2524 (a) (7) and, if the target is a
18 United States person, the certification or certifications
19 are not clearly erroneous on the basis of the statement
20 made under section 2524 (a) (7) (E) and any other
21 information furnished under section 2524 (c).
22 "(b) An order approving an electronic surveillance
23 under this section shall—
24 "(1) specify—

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(A) the identity, if known, or a description
2 of the target of the electronic surveillance;
3 "(B) the nature and location of the facilities or
4 the place at which the electronic surveillance will be
5 directed;
6 "(C) when the target of the surveillance is not
7 a foreign power as defined in section 2521 (b) (1)
8 (A), (B), or (C), the type of information sought
9 to be acquired and when the target is a foreign
10 power defined in section 2521 (b) (1) (A), (B), or
11 (C), the designation of the type of foreign intelli-
12 gence information under section 2521 (b) (5) sought
13 to be acquired;
14 "(D) when the target of the surveillance is not
15 a foreign power, as defined in section 2521 (b) (1)
16 (A), (B), or (C), the means by which the elec-
17 tronic surveillance will be effected, and when the
18 target is a foreign power, as defined in section 2521
19 (b) (1) (A), (B), or (C), a designation of the
20 type of electronic surveillance to be used according
21 to the categories described in section 2521 (b) (6)
22 and whether physical entry will be used to effect the
23 surveillance; and

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 "(E) the period of time during which the
2 electronic surveillance is approved; and
3 "(2) direct—
4 "(A) that the minimization procedures be
5 followed;
6 "(B) that, upon the request of the applicant, a
7 specified communication or other common carrier,
8 landlord, custodian, contractor, or other specified
9 person furnish the applicant forthwith any and all
10 information, facilities, or technical assistance, neces-
11 sary to accomplish the electronic surveillance in such
12 manner as will protect its secrecy and produce a
13 minimum of interference with the services that such
14 carrier, landlord, custodian, contractor, or other per-
15 son is providing that target of electronic surveillance;
16 "(C) that such carrier, landlord, custodian, or
17 other person maintain under security procedures
18 approved by the Attorney General and the Director
19 of Central Intelligence any records concerning the
20 surveillance or the aid furnished which such person
21 wishes to retain;
22 "(D) that the applicant compensate, at the
23 prevailing rate, such carrier, landlord, custodian, or
24 other person for furnishing such aid.
25 "(c) An order issued under this section may approve

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 an electronic surveillance not targeted against a foreign
2 power, as defined in section 2521 (b) (1) (A), (B), or
3 (C), for the period necessary to achieve its purpose, or for
4 ninety days, whichever is less; an order under this section
5 shall approve an electronic surveillance targeted against a
6 foreign power, as defined in section 2521 (b) (1) (A),
7 (B), or (C), for the period specified in the certification
8 required in section 2524 (a) (7) (F), or for one year, which-
9 ever is less. Extensions of an order issued under this chapter
10 may be granted on the same basis as an original order upon
11 an application for an extension made in the same manner as
12 required for an original application and after new findings
13 required by subsection (a) of this section. In connection
14 with applications for extensions where the target is not a for-
15 eign power, as defined in section 2521 (b) (1) (A), (B), or
16 (C), the judge may require the applicant to submit informa-
17 tion, obtained pursuant to the original order or to any previ-
18 ous extensions, as may be necessary to make new findings of
19 probable cause. The judge may assess compliance with the
20 minimization procedures required by this chapter.
21 "(d) Notwithstanding any other provision of this
22 chapter when the Attorney General reasonably determines
23 that—
24 "(1) an emergency situation exists with respect to
25 the employment of electronic surveillance to obtain for-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 eign intelligence information before an order authorizing
2 such surveillance can with due diligence be obtained, and
3 "(2) the factual basis for issuance of an order under
4 this chapter to approve such surveillance exists, he may
5 authorize the emergency employment of electronic sur-
6 veillance if a judge designated pursuant to section 2523
7 of this chapter is informed by the Attorney General or
8 his designate at the time of such authorization that the
9 decision has been made to employ emergency electronic
10 surveillance and if an application in accordance with this
11 chapter is made to that judge as soon as practicable, but
12 not more than twenty-four hours after the Attorney Gen-
13 eral authorizes such acquisition. If the Attorney General
14 authorizes such emergency employment of electronic
15 surveillance, he shall require that the minimization proce-
16 dures required by this chapter for the issuance of a judi-
17 cial order be followed. In the absence of a judicial order
18 approving such electronic surveillance, the surveillance
19 shall terminate when the information sought is obtained,
20 when the application for the order is denied, or after the
21 expiration of twenty-four hours from the time of au-
22 thorization by the Attorney General, whichever is earli-
23 est. In the event that such application for approval is
24 denied, or in any other case where the electronic sur-
25 veillance is terminated and no order is issued approving

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 the surveillance, no information obtained or evidence
2 derived from such surveillance shall be received in
3 evidence or otherwise disclosed in any trial, hearing,
4 or other proceeding in or before any court, grand jury,
5 department, office, agency, regulatory body, legislative
6 committee, or other authority of the United States, a
7 State, or political subdivision thereof; and no informa-
8 tion concerning any United States person acquired from
9 such surveillance shall subsequently be used or dis-
10 closed in any other manner by Federal officers or
11 employees without the consent of such person, except
12 with the approval of the Attorney General where the
13 information indicates a threat of death or serious bodily
14 harm to any person. A denial of the application made
15 under this subsection may be reviewed as provided
16 in section 2523.

17 **"§ 2526. Use of information**

18 "(a) Information concerning United States persons
19 acquired from an electronic surveillance conducted pursuant
20 to this chapter may be used and disclosed by Federal officers
21 and employees without the consent of the United States per-
22 son only for purposes specified in section 2521 (b) (8) (A)
23 through (F) and in accordance with the minimization pro-
24 cedures required by this chapter, or for the enforcement of
25 the criminal law if its use outweighs the possible harm to

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 the national security. No otherwise privileged communica-
2 tion obtained in accordance with, or in violation of, the
3 provisions of this chapter shall lose its privileged character.
4 No information acquired from an electronic surveillance
5 conducted pursuant to this chapter may be used or disclosed
6 by Federal officers or employees except for lawful purposes.
7 "(b) The minimization procedures required under this
8 chapter shall not preclude the retention and disclosure, for
9 law enforcement purposes, of any information which consti-
10 tutes evidence of a crime if such disclosure is accompanied
11 by a statement that such evidence, or any information de-
12 rived therefrom, may only be used in a criminal proceeding
13 with the advance authorization of the Attorney General.
14 "(c) Whenever the Government of the United States,
15 of a State, or of a political subdivision thereof intends to
16 enter into evidence or otherwise use or disclose in any trial,
17 hearing, or other proceeding in or before any court, depart-
18 ment, officer, agency, or other authority of the United
19 States, a State, or a political subdivision thereof, any infor-
20 mation obtained or derived from an electronic surveillance,
21 the Government shall prior to the trial, hearing, or other
22 proceeding or at a reasonable time prior to an effort to so
23 disclose or so use the information or submit it in evidence
24 notify the court in which the information is to be disclosed or
25 used or, if the information is to be disclosed or used in or

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 before another authority, shall notify a court in the district
2 wherein the information is to be so disclosed or so used that
3 the Government intends to so disclose or so use such infor-
4 mation.

5 "(d) Any person who has been the target of electronic
6 surveillance or whose communications or activities have been
7 subject to electronic surveillance and against whom evidence
8 derived from such electronic surveillance is to be, or has
9 been, introduced or otherwise used or disclosed in any trial,
10 hearing, or proceeding in or before any court, department
11 officer, agency, regulatory body or other authority of the
12 United States, a State, or a political subdivision thereof,
13 may move to suppress the contents of any communication
14 acquired by electronic surveillance, or evidence derived
15 therefrom, on the grounds that—

16 "(1) the communication was unlawfully acquired;
17 or

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

20 Such motion shall be made before the trial, hearing, or pro-
21 ceeding unless there was no opportunity to make such
22 motion or the person was not aware of the grounds of the
23 motion.

24 "(e) Whenever any court is notified in accordance with
25 subsection (c), or whenever a motion is made by an ag-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 grieved person pursuant to subsection (d), to suppress evi-
2 dence on the grounds that it was obtained or derived from an
3 unlawful electronic surveillance, or whenever any motion or
4 request is made by an aggrieved person pursuant to section
5 3504 of this title or any other statute or rule of the United
6 States, to discover, obtain, or suppress evidence or informa-
7 tion obtained or derived from electronic surveillance, the
8 Federal court, or where the motion is made before another
9 authority, a Federal court in the same district as the author-
10 ity, shall, notwithstanding any other law, if the Government
11 by affidavit asserts that disclosure or an adversary hearing
12 would harm the national security of the United States, re-
13 view in camera and ex parte the application, order, and other
14 materials relating to the surveillance as may be necessary to
15 determine whether the surveillance was authorized and con-
16 ducted in a manner that did not violate any right afforded by
17 the Constitution and statutes of the United States to the ag-
18 grieved person. In making this determination, the court shall
19 disclose to the aggrieved person portions of the application,
20 order, or other materials relating to the surveillance only
21 where such disclosure is necessary to make an accurate deter-
22 mination of the legality of the surveillance. If the court de-
23 termines that the electronic surveillance of the aggrieved
24 person was not lawfully authorized or conducted, the court
25 shall in accordance with the requirements of law suppress the

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 information obtained or evidence derived from the unlawful
2 electronic surveillance. If the court determines that the sur-
3 veillance was lawfully authorized and conducted, the court
4 shall deny any motion for disclosure or discovery unless re-
5 quired by due process.

6 "(f) If an emergency employment of the electronic
7 surveillance is authorized under section 2525 (d) and a sub-
8 sequent order approving the surveillance is not obtained, the
9 judge shall cause to be served on any United States person
10 named in the application and on such other United States
11 persons subject to electronic surveillance as the judge may
12 determine in his discretion it is in the interest of justice to
13 serve, notice of—

14 "(1) the fact of the application;

15 "(2) the period of the surveillance; and

16 "(3) the fact that during the period information
17 was or was not obtained.

18 On an ex parte showing of good cause to the judge the serv-
19 ing of the notice required by this subsection may be post-
20 poned or suspended for a period not to exceed ninety days.
21 Thereafter, on a further ex parte showing of good cause, the
22 court shall forego ordering the serving of the notice required
23 under this subsection.

24 "(g) In circumstances involving the unintentional
25 acquisition, by an electronic, mechanical, or other surveil-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 lance device of the contents of any radio communication,
2 under circumstances in which a person has a reasonable
3 expectation of privacy and a warrant would be required
4 for law enforcement purposes, and where both the sender
5 and all intended recipients are located within the United
6 States, such contents shall be destroyed upon recognition,
7 except with the approval of the Attorney General where the
8 contents indicate a threat of death or serious bodily harm
9 to any person.

10 **"§ 2527. Report of electronic surveillance**

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

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

18 "(2) the total number of such orders and exten-
19 sions either granted, modified, or denied.

20 **"§ 2528. Congressional oversight**

21 "(a) On a semiannual basis the Attorney General shall
22 fully inform the House Permanent Select Committee on In-
23 telligence and the Senate Select Committee on Intelligence
24 concerning all electronic surveillance under this chapter.
25 Nothing in this chapter shall be deemed to limit the author-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 ity and responsibility of the appropriate committees of each
2 House of Congress to obtain such additional information as
3 they may need to carry out their respective functions and
4 duties.

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

13 SEC. 3. The provisions of this Act and the amendment
14 made hereby shall become effective upon enactment: *Pro-*
15 *vided,* That any electronic surveillance approved by the
16 Attorney General to gather foreign intelligence information
17 shall not be deemed unlawful for failure to follow the proce-
18 dures of chapter 120, title 18, United States Code, if that sur-
19 veillance is terminated or an order approving that surveillance
20 is obtained under this chapter within ninety days following
21 the designation of the first judge pursuant to section 2523 of
22 chapter 120, title 18, United States Code.

23 SEC. 4. Chapter 119 of title 18, United States Code, is
24 amended as follows:

25 (a) Section 2511 (1) is amended—

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 (1) by inserting "or chapter 120 or with respect to
2 techniques used by law enforcement officers not involv-
3 ing the interception of wire or oral communications
4 as otherwise authorized by a search warrant or order of
5 a court of competent jurisdiction," immediately after
6 "chapter" in the first sentence;
7 (2) by inserting a comma and "or, under color of
8 law, willfully engages in any other form of electronic
9 surveillance as defined in chapter 120" immediately
10 before the semicolon in paragraph (a);
11 (3) by inserting "or information obtained under
12 color of law by any other form of electronic surveillance
13 as defined in chapter 120" immediately after "contents
14 of any wire or oral communication" in paragraph (c);
15 (4) by inserting "or any other form of electronic
16 surveillance, as defined in chapter 120," immediately
17 before "in violation" in paragraph (c);
18 "(5) by inserting "or information obtained under
19 color of law by any other form of electronic surveillance
20 as defined in chapter 120" immediately after "any wire
21 or oral communication" in paragraph (d); and
22 (6) by inserting "or any other form of electronic
23 surveillance, as defined in chapter 120," immediately
24 before "in violation" in paragraph (d).
25 (b) (1) Section 2511 (2) (a) (i) is amended by insert-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 ing the words "or radio communication" after the words
2 "wire communication" and by inserting the words "or other-
3 wise acquire" after the word "intercept".

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

13 "(1) an order signed by the authorizing judge certi-
14 fying that a court order directing such assistance has
15 been issued; or

16 "(2) in the case of an emergency interception or
17 electronic surveillance as provided for in section 2518
18 (7) of this chapter or section 2525 (d) of chapter 120,
19 a certification under oath by the investigative or law
20 enforcement officer that the applicable statutory require-
21 ments have been met,

22 and setting forth the period of time for which the electronic
23 surveillance is authorized and describing the facilities from
24 which the communication is to be acquired. Any violation of
25 this subsection by a communication common carrier or an

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 officer, employee, or agency thereof, shall render the carrier
2 liable for the civil damages provided for in section 2520. No
3 communication common carrier or officer, employee, or
4 agent thereof shall disclose the existence of any interception
5 under this chapter or electronic surveillance, as defined in
6 chapter 120, with respect to which the common carrier
7 has been furnished either an order or certification under
8 this subparagraph, except as may otherwise be lawfully
9 ordered.".

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

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

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

20 "(e) Notwithstanding any other provision of this title
21 or section 605 or 606 of the Communications Act of 1934,
22 it shall not be unlawful for an officer, employee, or agent of
23 the United States in the normal course of his official duty
24 under procedures approved by the Attorney General to

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 conduct electronic surveillance as defined in section 2521
2 (b) (6) of chapter 120 without a court order for the sole
3 purpose of:

4 "(i) testing the capability of electronic equipment,
5 provided that no particular United States person shall
6 be intentionally targeted for testing purposes without
7 his consent, the test period shall be limited in extent
8 and duration to that necessary to determine the capabil-
9 ity of the equipment, that the content of any communica-
10 tion acquired under this paragraph shall be retained
11 and used only for the purpose of determining the ca-
12 pability of such equipment, shall be disclosed only to the
13 persons conducting the test, and shall be destroyed upon
14 completion of the testing, and that the test may exceed
15 ninety days only with the prior approval of the Attorney
16 General; or

17 "(ii) determining the existence and capability of
18 electronic surveillance equipment being used unlawfully,
19 provided that no particular United States person shall
20 be intentionally targeted for such purposes without his
21 consent, that such electronic surveillance shall be limited
22 in extent and duration to that necessary to determine
23 the existence and capability of such equipment, and that
24 any information acquired by such surveillance shall be

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 used only to enforce this chapter or section 605 of the
2 Communications Act of 1934 or to protect information
3 from unlawful electronic surveillance.
4 "(f) Nothing contained in this chapter, or section 605
5 of the Communications Act of 1934 (47 U.S.C. 605) shall
6 be deemed to affect the acquisition by the United States
7 Government of foreign intelligence information from inter-
8 national or foreign communications by a means other than
9 electronic surveillance as defined in section 2521 (b) (6)
10 of this title; and the procedures in this chapter and chapter
11 120 of this title, shall be the exclusive means by which
12 electronic surveillance, as defined in section 2521 (b) (6)
13 of chapter 120, and the interception of domestic wire and
14 oral communications may be conducted.".
15 (d) Section 2511 (3) is repealed.
16 (e) Section 2515 is amended by inserting the words
17 "or electronic surveillance, as defined in chapter 120, has
18 been conducted" after the word "intercepted", by inserting
19 the words "or other information obtained from electronic
20 surveillance, as defined in chapter 120," after the second
21 appearance of the word "communication", and by inserting
22 "or chapter 120" after the final appearance of the word
23 "chapter".

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 (f) Section 2518 (1) is amended by inserting the words
2 "under this chapter" after the word "communication".
3 (g) Section 2518 (4) is amended by inserting the
4 words "under this chapter" after both appearances of the
5 words "wire or oral communication".
6 (h) Section 2518 (9) is amended by striking the word
7 "intercepted" and inserting the words "intercepted pursuant
8 to this chapter" after the word "communication".
9 (i) Section 2518 (10) is amended by striking the word
10 "intercepted" and inserting the words "intercepted pursuant
11 to this chapter" after the first appearance of the word "com-
12 munication".
13 (j) Section 2519 (3) is amended by inserting the
14 words "pursuant to this chapter" after the words "wire or
15 oral communications" and after the words "granted or
16 denied".
17 (k) Section 2520 is amended by deleting all below
18 subsection (2) and inserting in lieu thereof: "Any person
19 other than a foreign power or an agent of a foreign power
20 as defined in sections 2521 (b) (1) and 2521 (b) (2) (A)
21 of chapter 120, who has been subject to electronic surveil-
22 lance, as defined in chapter 120, or whose wire or oral com-

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

1 munciation has been intercepted, or about whom information
2 has been disclosed or used, in violation of this chapter, shall
3 (1) have a civil cause of action against any person who so
4 acted in violation of this chapter and".

Passed the Senate April 20 (legislative day, February 6), 1978.

Attest: J. S. KIMMITT,
Secretary.

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4

95TH CONGRESS
2D SESSION

S. 1566

AN ACT

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.

APRIL 24, 1978

Referred to the Committee on the Judiciary

Approved For Release 2005/11/23 : CIA-RDP80S01268A000500040010-4