FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

HEARINGS

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND THE RIGHTS OF AMERICANS

OF THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

NINETY-FIFTH CONGRESS

SECOND SESSION

ON

S. 1566

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

JULY 19, 21, 1977 AND FEBRUARY 8, 24, 27, 1978

Printed for the use of the Select Committee on Intelligence

U.S. GOVERNMENT PRINTING OFFICE
94-628 WASHINGTON : 1978

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402
Stock Number 052-070-04477-2

SENATE SELECT COMMITTEE ON INTELLIGENCE

(Established by S. Res. 400, 94th Cong., 2d sess.)

DANIEL K. INOUYE, Hawaii, *Chairman*
BARRY GOLDWATER, Arizona, *Vice Chairman*

BIRCH BAYH, Indiana
ADLAI E. STEVENSON, Illinois
WILLIAM D. HATHAWAY, Maine
WALTER D. HUDDLESTON, Kentucky
JOSEPH R. BIDEN, Jr., Delaware
ROBERT MORGAN, North Carolina
GARY HART, Colorado
DANIEL PATRICK MOYNIHAN, New York

CLIFFORD P. CASE, New Jersey
JAKE GARN, Utah
CHARLES McC. MATHIAS, Jr., Maryland
JAMES B. PEARSON, Kansas
JOHN H. CHAFEE, Rhode Island
RICHARD G. LUGAR, Indiana
MALCOLM WALLOP, Wyoming

ROBERT C. BYRD, West Virginia, *Ex Officio Member*
HOWARD H. BAKER, Jr., Tennessee, *Ex Officio Member*

WILLIAM G. MILLER, *Staff Director*
EARL D. EISENHOWER, *Minority Staff Director*
AUDREY H. HATRY, *Chief Clerk*

SUBCOMMITTEE ON INTELLIGENCE AND THE RIGHTS OF AMERICANS

BIRCH BAYH, Indiana, *Chairman*
JAKE GARN, Utah, *Vice Chairman*

ROBERT MORGAN, North Carolina
DANIEL PATRICK MOYNIHAN, New York

CLIFFORD P. CASE, New Jersey
JOHN H. CHAFEE, Rhode Island

CONTENTS

HEARING DAYS

LIST OF WITNESSES

TUESDAY, JULY 19, 1977

THURSDAY, JULY 21, 1977

WEDNESDAY, FEBRUARY 8, 1978

APPENDIXES

MATERIAL FOR THE RECORD

S. 1566

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

TUESDAY, JULY 19, 1977

U.S. SENATE,
SUBCOMMITTEE ON INTELLIGENCE
AND THE RIGHTS OF AMERICANS
OF THE SELECT COMMITTEE ON INTELLIGENCE,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:01 a.m., in room 6226, Dirksen Senate Office Building, Senator Birch Bayh (chairman of the subcommittee) presiding.

Present: Senators Bayh (presiding), Inouye, Hathaway, Huddleston, Morgan, Hart, Garn, and Chafee.

Also present: William G. Miller, staff director; Audrey Hatry, chief clerk of the committee.

Senator BAYH. We will convene our hearings. Our full committee chairman is en route, and pending his arrival, perhaps I would ask the Attorney General's indulgence for a brief opening statement to try to put the foundation on what we are doing and why we are here, and I will ask my colleague from North Carolina and other colleagues if they care to also have any opening comments.

The Subcommittee on Intelligence and the Rights of Americans of the Senate Select Committee on Intelligence is today beginning hearings on S. 1566, the Foreign Intelligence Surveillance Act of 1978. Our first witness is the distinguished Attorney General Griffin Bell, and Mr. Attorney General, as busy as you are, we appreciate that you and your top staff people would take time to be with us here. I know from the discussions we have had, really from our first meeting, of your intense interest in resolving this problem, and I think what you have done while Attorney General means that the words you spoke during your confirmation hearings were words of substance and not words of rhetoric. Those of us who knew you had no doubt, and hopefully some of the doubting Thomases have had their doubts removed.

The hearings will continue on Thursday, July 21, when we will hear from the Director of Central Intelligence and representatives of the Departments of State and Defense. An additional hearing is scheduled for Monday, August 1,* to receive testimony from outside witnesses and representatives of interested groups. All the members of the full committee have been invited to participate in these hearings.

*This hearing was cancelled and took place Wednesday, February 8, 1978.

Because some aspects of foreign intelligence surveillance will require the discussion of classified information, the subcommittee intends to take further testimony from administration witnesses in executive session. These will include representatives of the Department of State, Department of Defense, Justice Department, the FBI, the CIA, and the National Security Agency.

The subcommittee is taking up the bill before the Judiciary Committee has reported it because of the importance of completing our hearings by the August recess. I will say to my colleagues of the committee I have discussed this with the chairman of the Judiciary Committee and both of the ranking members of the subcommittee that is considering this, and they are glad that we are moving as rapidly as we are.

We anticipate that the Judiciary Committee will report the bill, with some modifications, before our hearings are over. Until then, the subcommittee will examine the act in the form it was originally introduced.

This bill is an important first step towards full-scale legislative regulation of the intelligence activities of our country. We hope to furnish to the people of our country the kind of legislative charter, the kind of wiretap legislation that they have every right to deserve, and we hope to finish our considerations of this bill promptly so that the committee can move on to deal with further measures not only to clarify the authority and structure of the intelligence community, but also to place clear legal limits on the full range of intelligence activities which may affect the rights of Americans.

One of the main subjects we have asked the Attorney General to address is whether this act could be amended to cover surveillance of U.S. persons abroad. The present bill protects Americans only when they are in the United States, and there are no minimization procedures to limit the use of information about Americans acquired indirectly from international and foreign communications.

We have also asked the Attorney General to discuss with us the practical consequences of the act, the standards and procedures contemplated for making the Executive certifications required by the act, and appropriate procedures for congressional oversight. An additional matter of concern to the subcommittee is the circumstances in which the information acquired about Americans who are not targets of surveillance may nevertheless be used or disseminated.

Other questions involve the relationship of the act to the Vienna Convention, and to the legal and human rights obligations of the United States toward foreign visitors in this country.

Last year, as all members of this committee know, the Intelligence Committee reported a similar bill, S. 3197, which failed to reach the Senate floor. During the Attorney General's confirmation hearings, I asked about the possibility of the administration supporting a new bill with changes designed to resolve the misgivings some of us had about the original bill. A number of areas for improvement were discussed with officials of the Justice Department. The bill before us today incorporates at least in part three significant changes proposed in those discussions.

The most important change is the extension of the bill, and the court order requirement, to targeting of the international communica-

tions of Americans who are in the United States. I might point out this is a very important feature that was not covered in the bill last year. For the first time, now, targeting of international communications of Americans who are in the United States is covered in this bill.

A second significant improvement is judicial review of the executive certification that surveillance of an American is necessary to obtain foreign intelligence information. Third, the bill states clearly that its standards and procedures are the exclusive means by which electronic surveillance as defined in this act may be conducted. There is no exception for the President to authorize such surveillance on his own for matters that were not contemplated by Congress, and I think it speaks well of the President of the United States. For the first time, to my knowledge, in history we have a President of the United States who does not claim implied authority, but sends his right arm, the Attorney General of the United States, up here to support and indeed to help in drafting of legislation which governs the exclusive means by which Presidential authority may be exercised in this very controversial yet critical area.

However, and here again I speak, I guess, just in my judgment, but as one who has studied this over a couple or 3 years, I just want to say that even though this loophole is now closed for the surveillance covered by this bill, in my judgment there is still room for the President to claim inherent authority to target Americans abroad for surveillance and to use information about Americans acquired directly from surveillance of international communications. Until Congress enacts legislation in this area, the foreign intelligence surveillance activities of the Executive branch will continue to raise serious problems for the rights of Americans.

I think it is important for us to look at how we can make what I think is a much better bill an even better bill, and I want to thank you again, Mr. Attorney General, and your assistants for their close cooperation with the committee during the development of this bill. We have not yet resolved all of our differences, and sometimes the Justice Department must represent the views of other agencies as well as its own position, but it has been a privilege to have a chance to develop the kind of working relationship we have had.

We are all aware of the delicate combination of interests that bring us together. Nobody is naive enough to not understand the need to have good, efficient, honest intelligence gathering agencies that have the best expertise available to protect us from those who would take away our freedom, but certainly in this day and age we don't need to be reminded that it is equally important for us to give those tools and provide that framework to those who serve our intelligence community in a manner that also protects the rights of individual Americans.

This is supposed to be and I firmly believe it is one of the real distinctions between our society and others, that we are able to meet the needs of the Government as a whole without transgressing on the rights of individual American citizens, and it is to that goal that this committee is working, and I am sure the Attorney General is equally dedicated.

Could I ask my colleague from Kentucky if he has opening remarks he would like to make at this time?

Senator HUDDLESTON. Thank you, Mr. Chairman. I would like to join you and the other members in welcoming the Attorney General, Mr. Bell, to the opening day of hearings by the Senate Select Committee on Intelligence on the Foreign Intelligence Surveillance Act of 1977. Now, this bill has generated considerable discussion, as we all know, and in many ways is a product of congressional investigations of our intelligence agencies. The abuses which were discovered in the area of warrantless wiretaps made clear the necessity for legislative action, and unlike many previous administrations, the Ford administration, particularly Attorney General Levy, the Carter administration, particularly Attorney General Bell, have worked closely with the Congress in fashioning corrective legislation.

I would like the record to show my appreciation for the work of these two administrations and for the leadership shown by the distinguished senior Senator from Indiana, the chairman of the Senate Select Committee's Subcommittee on Intelligence and the Rights of Americans, along with Senator Garn, the vice chairman of the Subcommittee on Intelligence and the Rights of Americans. He has done a masterful job in preparing legislation in this area. He did so last year, and his work this year has led to a number of improvements in the bill that is before us as he himself detailed.

Now, the abuses which have led to the presentation of this legislation were the result of actions taken on the basis of claims of inherent Presidential power. Like so many other fields or other areas in the field of intelligence, there was no legislative guidance for the officials of our intelligence community. Neither the need to surveil Americans for foreign intelligence purposes nor the procedures to be followed were ever established by Congress, and I believe that it is important that Congress now make such determinations, striking a balance between the need to protect our national security and the need to protect the rights of Americans.

This legislation is the first piece of charter legislation for the intelligence community, and is the first of many which will be brought before the Select Committee. Other legislation which I intend to introduce during the session will provide a charter for what is now the Director of Central Intelligence, as well as charters for the CIA, the NSA, and the domestic security activities of the FBI. Special care will be taken to protect the rights of Americans. At the same time, the need for strengthening our vital intelligence agencies will be given the utmost attention.

So, because of the importance of this bill and because of its strong ties to other charter legislation that is now being reviewed by the Subcommittee on Charters and Guidelines, I am looking forward with great interest to hearing the Attorney General this morning, and I appreciate the opportunity, Mr. Chairman, to participate in the Committee's activities.

Senator BAYH. I will say to my distinguished colleague from Kentucky, I appreciate your thoughtful observations relative to the Senator from Indiana, and it has been a privilege, I think, to see this committee work together and to understand the need to have a close relationship between its subcommittees and the missions that we are carrying, and the importance of establishing charters on which our intelligence activities can be based cannot be exaggerated as far as its importance is concerned, and indeed, it is in good hands.

Does the distinguished Senator from North Carolina care to get us off to a good start this morning?

Senator MORGAN. Mr. Chairman, just a word. Judge Bell, where I am from, we are not used to opening statements in court. We go ahead and try a case and then take the last speech to the jury, but it is not often I have a chance to lecture the Attorney General of the United States, so I might as well take advantage of it.

Judge Bell, I have some apprehensions about this bill. I might just say by way of introduction that when I came to the Senate 2½ years ago, I guess you could have classified me as a rather conservative, staunch law and order man, having come from a position as attorney general of my State, and head of a department in which I had the State Bureau of Investigation, and I had a great deal of respect for Federal law enforcement agencies.

To be sure, I complained about the lack of cooperation between the Federal Bureau and the local law enforcement agencies, but that, I think, was to be expected, but after sitting through months, weeks and months and almost years, a year and a half of hearings about the intelligence agencies, and when I say that I include all of them, I have become dubious of everything we do, and perhaps too much so. I was one of those who did not vote for the wiretap bill that was before this committee last year. I had a number of reservations about it.

First of all, the seven judges, it seemed to me, left room to do a little judge shopping if you wanted to. Second, as I recall it, there was no real provision for the judges to look back of the certification to see whether or not the certification was based upon reasonable or probable—facts. Let's put it that way rather than getting into the probable cause area.

I was disturbed about the lack of criminal standards. One of the things I was disturbed about was the statement which could have been interpreted as recognizing the inherent power of the Presidency to wiretap in terms of national security, and of course some of those things have been eliminated, but as I have studied your testimony before the Judiciary Committee, and as I have studied other matters before me, and I have got more here than I can study, I just want to say that each time I keep coming back, time after time after time again, to the statement that was attributed to Attorney General Harlan Stone in 1924, and the more I am convinced, the more I see, the more I hear, the more I am convinced that Justice Stone was right, and that maybe we ought to stick to that guideline, and if we can't stick to it with the present state of the criminal laws, maybe we ought to change the criminal laws.

At the risk of being repetitious, I just want to read this one statement, because I have made a conscientious effort to read everything that I can about this, and every time I think I have reconciled myself to these new theories, and new thresholds, I find myself coming right back to what he had to say, and here is what he had to say.

There is always a possibility that a secret police may become a menace to free government and free institutions, because it carries with it the possibility of abuses of power which are not always quickly apprehended or understood.

We found that out, that many of the things, abuses that we are learning now in all of the agencies that took place years ago, they were not quickly apprehended.

"It is important," he said, "that activities be strictly limited to performance of those functions for which it was created, and that its agents themselves be not above the law or beyond its reach." The Bureau of Investigation is not concerned with political or other opinions of individuals. It is concerned only with our 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 the human liberty which should be our first concern to cherish, and that is where I start from.

If you have anything that you could help persuade me of the correctness, or that this bill is better, I would be glad to hear from you as we go along. Thank you.

Senator BAYH. Thank you, Senator Morgan. As I have said to you, sir, I, too, have struggled with the criminal standards test, and I want to come down foursquare where you just put us. I finally was able to resolve this in my own mind with a very carefully drawn exception, but that was a part of the negotiating process, not a matter of first wishes, and I appreciate your bringing our attention to this matter. We cannot overemphasize it.

Senator MORGAN. When I think I have it resolved, I wake up the next morning and it is not.

Senator BAYH. I have gone through that same kind of sleep-and-awake process. We appreciate the fact that as busy as our full committee chairman is, that he has had the opportunity to get with us at the start of our hearings. Senator Inouye, do you have some opening comments that we might share this morning?

CHAIRMAN INOUYE. I just would like to welcome our Attorney General and thank him for his cooperation. General, your staff has been extremely cooperative with the committee and we are very grateful for that. I think with this spirit of cooperation this matter should be law soon.

Senator BAYH. I should note that a distinguished ranking member of our subcommittee, Senator Garn, had every intention of being here this morning. He got caught up in some emergency problems like we all have on occasion. I understand he will be along shortly, as quickly as he can get here, and we are looking forward to his being here.

Also, Senator Biden has submitted a statement that he would like included in the record, along with his additional views on S. 3197, which our full committee considered in the last Congress. Without objection, they will be inserted in the record at this point.

[The statement of Senator Biden along with his additional views regarding S. 3197, 94th Congress, follow:]

STATEMENT OF SENATOR BIDEN AND ADDITIONAL VIEWS ON S. 3197

I welcome the hearings that begin today on S. 1566, the Carter administration's electronic surveillance legislation. I view S. 1566 as a substantial improvement over S. 3197, similar legislation proposed by President Ford in the last Congress.

Last year I was a member of this Subcommittee and spent considerable time with the Chairman and other members attempting to bring S. 3197 into line with

our view of the Fourth Amendment. The Committee adopted, with a few modifications, an amendment I proposed to S. 3197 that would have created a more precise standard for the use of electronic surveillance in national security cases a standard more consistent with the Fourth Amendment. I am pleased to see that much of that language remains in the present legislation.

When S. 3197 was reported from the Select Committee last summer, I voted in favor of reporting the bill but I expressed my lack of enthusiasm in additional views. I ask unanimous consent that those additional views be reprinted at this point in the Subcommittee's record. I ask that those views be incorporated because they summarize many of my present concerns with the legislation.

In brief I mentioned three basic areas which I thought required additional attention and which served as the basis of my objection to hasty consideration of the legislation. Those concerns were as follows: (1) The constitutionality of the legislation; (2) the "inherent authority" provision; and, finally, (3) the impact of the legislation upon legislative charters to be drafted by the Committee.

As the result of negotiations between the Committee, the staff and the Intelligence Community, substantial progress was made in the last year. The legislation eliminates the so-called "inherent authority" provision of S. 3197 and covers NSA intercepts, an idea which I and other critics of the bill proposed in the last Congress.

The new legislation does not, however, resolve my concerns about its constitutionality. As I pointed out in my statement last summer, the Fourth Amendment has basically two components in its protection of the privacy of Americans. First, a citizen's privacy cannot be invaded unless a judicial officer issues a warrant authorizing a search and second, the judge must have probable cause to believe the search will seize particular evidence of criminal activity. Unfortunately the focus of the debate over the constitutionality of this legislation has been upon the first element of the Fourth Amendment—whether or not a warrant need be required. In expanding the warrant requirement to NSA intercepts and eliminating the so-called "inherent authority" exception, many believe the constitutional problems with this legislation have been solved. As I pointed out last summer, and as I reiterate today, I do not believe the constitutional issues have been totally resolved until the second element of the Fourth Amendment has been addressed. So long as this legislation permits interception of private conversations where the judge has not required the government to prove that specific evidence of crime will be seized, then I believe the legislation is constitutionally defective.

I still have doubts about proceeding with legislation such as this which addresses only one basic technique used by the Intelligence Community before it has developed legislation which charters the Intelligence Community to conduct investigations in the first instance. In adopting legislation such as this, out of context, the Committee and the Congress might prejudice their efforts to regulate the use of informants, physical surveillance and other necessary intrusive techniques. This Committee has still not formally proposed its legislative charters for the Intelligence Community and, therefore, I still feel the wiretap bill should be a second priority to the development of those charters.

Finally, last summer I pointed out that at the same time we were attempting to clarify the responsibilities of national securities agencies, that we would also attempt to modernize statutes such as the Espionage Statute which control the behavior of private persons who might in some way jeopardize the national security. At the heart of this concern was the debate which raged last summer over application of electronic surveillance to unwitting U.S. citizens who might violate some old vague criminal statute or violate no statute but simply be engaged in communications with a foreign agent. In the course of my study of the problem of secrecy in the Intelligence Community in my capacity as chairman of the Secrecy Subcommittee, I have become increasingly aware of this problem. I have found that our espionage statutes and other statutes relating to the use of classified information are exceedingly vague. Ambiguities in these statutes are a threat not only to civil liberties but to national security. Basing electronic surveillances upon a violation of these statutes doesn't seem a particularly wise course at this time.

Since last summer and as a result of my work on the Secrecy Subcommittee, I have become increasingly aware that the problem of secrecy and concern in the Intelligence Community over protecting sources and methods has a way of undercutting the equal and just enforcement of the criminal laws. I have discovered

cases in which the Intelligence Community's overriding concern for secrecy has led them to forego legitimate espionage investigations and other enforcement of the criminal statutes out of fear that sensitive information might be disclosed in the course of criminal trials. I am aware that this basic issue has been touched upon in the course of negotiations over S. 1566. For example, there are sections of this legislation that deal with the requirement that the Intelligence Community disclose to judges passing on warrants information relevant to the request for electronic surveillance.

Since the Secrecy Subcommittee will be looking further at many of these same issues, it is of some concern to me that the Committee is proceeding with legislation which may in some way prejudice our inquiry. This latter point is just one more reason why this Committee should be exceedingly careful in processing this legislation and should make it clear to the Executive Branch and in particular to the Intelligence Community that although we are taking positions on matters that have an impact on other parts of our work we do not intend them to prejudice positions we might take on subsequent legislation.

In conclusion, I view this legislation in much the same light as I did S. 3197 after it had been processed by this Committee last summer. It is a substantial improvement over its predecessors. However, I am not sure whether it is an adequate improvement over existing law. I, therefore, will work to improve it within this Committee and will reserve the right to vote against the bill when it comes up in this Committee and, if necessary, when it reaches the Floor.

Additional Views of Senator Biden on S. 3197

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

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

I. The constitutionality of S. 3197

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

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

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

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

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

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

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

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

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

II. THE INHERENT AUTHORITY SECTION

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

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

Unfortunately, it may be impossible to write language on this matter which is neutral in effect. Congress is on notice of NSA abuses, including project SHAMROCK and the watchlists both documented by the Church Committee. Congress is on notice of the myriad of abuses engaged in by other intelligence agencies and by non-intelligence officials, in the course of the Watergate matter, undertaken in the name of this doctrine. For Congress to act in this area and

deliberately skirt NSA and at the same time leave undisturbed inherent authority may be viewed by some courts as sanctioning the doctrine.

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

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

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

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

Unfortunately, we have not had time to have a comprehensive staff or agency briefing on the so-called counterintelligence and positive intelligence activities of the Federal government within the United States. Specifically, we have not carefully examined the existing statutory authority for such activities. We know, indeed Attorney General Levi has admitted, that there are not adequate statutes for their present programs. This is the reason why we have had to authorize, in the revised definitions of S. 3197, electronic surveillance of Americans not engaged in criminal activities.

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

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

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

"28 U.S.C. 533. Investigative and other officials; Appointment

"The Attorney General may appoint officials—

"(1) to detect and prosecute crimes against the United States;

"(2) to assist in the protection of the person of the President; and

"(3) to conduct such other investigations regarding official matters under the control of the Department of Justice and the Department of State as may be directed by the Attorney General."

This section does not limit the authority of departments and agencies to investigate crimes against the United States when investigative jurisdiction has been assigned by law to such departments and agencies.

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

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

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

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

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

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

Mr. Attorney General, I think we have vented our spleen moderately here this morning, and now why don't we get down to the reason for being here? We would like to hear your thoughts on this legislation.

TESTIMONY OF GRIFFIN B. BELL, ATTORNEY GENERAL OF THE UNITED STATES; ACCOMPANIED BY JOHN M. HARMON, ASSISTANT ATTORNEY GENERAL, OFFICE OF LEGAL COUNSEL; FREDERICK D. BARON, SPECIAL ASSISTANT TO THE ATTORNEY GENERAL; AND WILLIAM FUNK, OFFICE OF LEGAL COUNSEL

Attorney General BELL. Senator Bayh, Chairman Inouye, Senator Huddleston, and Senator Morgan, I have a very short statement. It would probably be more productive to have a question-and-answer

session. I know many of you have questions. That has come out in your opening statements. So, I will read this short statement, and then try to answer questions.

I am pleased to appear before you 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.

I wish to take this opportunity to thank this committee for holding these hearings promptly, without waiting for the Judiciary Committee's report of the bill. Given the crowded legislative docket facing the Senate, if S. 1566 is to pass the Senate this session, the same spirit of cooperation between the Administration and Congress, and indeed within Congress, which has been demonstrated thus far must continue.

Except for one matter, which I know concerns several of the members of this committee, I would like to submit my prepared statement before the Judiciary Committee as my prepared statement before this committee.

Senator BAYH. Without objection, it is so ordered.

[The prepared statement of Hon. Griffin B. Bell follows:]

PREPARED STATEMENT OF HON. GRIFFIN B. BELL, ATTORNEY GENERAL OF THE UNITED STATES, BEFORE THE SENATE JUDICIARY COMMITTEE, SUBCOMMITTEE ON CRIMINAL LAWS AND PROCEDURES

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, and 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 guarantee our nation's security on the one hand, and the preservation of basic human rights on the other." It is a very delicate balance to strike, but one which is necesary in our society, and a balance which cannot be achieved by sacrificing either our nation's security or our civil liberties. In my view this bill strikes the balance, sacrifices neither our security nor our civil liberties, and assures that the abuses of the past will remain in the past and that the dedicated and patriotic men and women who serve this country in intelligence positions, often under substantial hardships and even danger, will have the affirmation of Congress that their activities are proper and necessary.

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 terrorist activities for or on 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 clandestine 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 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 United States 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-frisks and airport searches. In the case of *United States v. United States District Court* 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 (ii) 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-United States 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 equipment 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 safeguard 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 responsibility of the Government in conducting intelligence activities.

Attorney General BELL. Thank you. The one matter not covered in detail in that statement is the question of extending S. 1566 to cover all U.S. Government surveillances worldwide.

Before S. 1566 was introduced, the administration seriously considered proposing a bill which would cover all electronic surveillances, not just those within the United States. Because the work on a bill limited to surveillance in the United States was already far advanced and because there was a desire to enact legislation on this subject as soon as possible, it was decided not to attempt to expand the bill to cover overseas surveillances. It was expected to take several months to iron out the problems which are unique to overseas surveillances, and such a delay would have doomed any hope of legislation on electronic surveillance this year.

At the time S. 1566 was introduced, the administration announced that it would undertake, in cooperation with interested Members of Congress, to draft separate legislation covering overseas surveillance. We have been engaged in that task for almost 2 months, and the issues are still not resolved within the executive branch.

This is due to the number and complexity of the problems uniquely involved in overseas surveillances, and the difficulty in creating and maintaining meaningful safeguards in light of those problems.

While I am not prepared to go into great detail over these problems here, some of which could only be discussed in executive session, I can say that many of the problems arise out of the fact that overseas there is a fair degree of cooperation between our Government and the police

and intelligence services of other nations, and surveillances undertaken are not exclusively for our purposes. The level of cooperation in surveillances, moreover, can span the entire spectrum from situations where we effectively can control all aspects of the surveillance to situations where we have virtually no control.

Restrictions or limitations on such surveillances could result in the loss of cooperation. These cooperative ventures would require adjustments of one form or another in all aspects of S. 1566, if it were to be used as the vehicle for reaching overseas surveillances. It will not be a simple matter to apply to electronic surveillances abroad the provisions of S. 1566 relating to the standards for approval, the information to be given to the judge, and the limitations in the order itself.

A separate problem, not directly related to the joint operation problem is the standard under which Americans may be made the target of a surveillance. Under S. 1566 in almost all cases an American will have to be violating Federal law to be targeted for electronic surveillance. Yet in most cases our laws do not have extraterritorial effect, so that activity in the United States which would violate our laws would not be a violation if committed abroad. Even more problematic is the fact that overseas there may be a need for electronic surveillance against Americans for positive foreign intelligence purposes, as opposed to counterintelligence purposes.

An easy example is the American citizen who emigrates or defects to another country and rises to a position of power and influence in a foreign government.

In dealing with these problems one must keep in mind that overseas the foreign intelligence need for electronic surveillance is probably more critical than within the United States. The conditions under which our personnel must operate can include clandestine activities in hostile areas and often involves activities where our ability to engage in electronic surveillance at all is extremely fragile, because it must be covertly conducted in territory not under our control.

In raising these problems, however, I do not mean to suggest that they are unsurmountable. I do not believe they are. I mention them only to illustrate what I believe to be the inadvisability of attempting to cover overseas surveillance in S. 1566. It just cannot be done by means of a few simple amendments. The yet unresolved problems, some of which I have mentioned, suggest that if S. 1566 were to be delayed pending their resolution, there would be no legislation this session.

I am, therefore, restating the administration's commitment to draft separate legislation providing safeguards for Americans abroad from electronic surveillance by this Government for both intelligence and law enforcement purposes. I cannot provide a date by which such legislation will be ready, because it depends in part upon the resolution of some difficult policy problems. I can pledge, however, to move forward with my part of this project as expeditiously as I can responsibly do so.

My staff has already reported to me on productive meetings that have been held with the staff of this committee on this subject. In closing, I urge that this issue not be allowed to cause delay of the passage of S. 1566.

I know, Mr. Chairman, there are a lot of questions, and I will do my best to answer them. I have brought my brains along with me to fill the breach where I fail, so I have John Harmon and Frederick Baron and William Funk on my staff who work in this area. John Harmon is the head of the Office of Legal Counsel.

Senator BAYH. Thank you, Mr. Attorney General. We recognize the presence of your able assistants. Fortunately for them, you brought your own brains as well as the ones you referred to seated on either side of you. [Laughter.]

Let me pursue the one major point that you mentioned in your statement. You know in the deliberations we had prior to the introduction of the bill I expressed a willingness, the desire, really, to cooperate so we could move the best possible bill. I did express concern, both an obligation to try to look more carefully, more definitively at this particular problem than you were prepared to, understandably.

Now, you mentioned the example of an American who might be in hostile territory, our agents would be operating in hostile territory, thus it would be difficult to utilize the same kind of standard abroad as it is to be utilized in the United States. It would be helpful if we differentiated. This is not unique in the way our Government has tried to govern its response to problems in the collection of intelligence, governing intelligence, to try to separate out some countries where it might be more difficult to operate than others, and in those countries where we have a close working relationship, part of a mutual reliance and support mutual principles, we would require the same standards as we require in our own country, but in other countries that would meet the definition that you describe. hostile territory, however you might want to describe it, I don't think we want to get into that here, but would it be possible to differentiate on that basis to help resolve some of the problems that you might see?

Attorney General BELL. That is possible. I have not been working with my committee on this bill. My interest in protecting American citizens overseas stems from the conversations we had at my Senate confirmation hearings. When Vice President Mondale and I took this legislation to the President, we told him we were both committed to some protection for Americans overseas, and that when he announced the administration's support of this particular bill, we would appreciate him saying that we were going to move forward immediately on some protection for overseas Americans—Americans who happened to be overseas.

I had people working on this problem even before that time. I have not reviewed all of the problems and obstacles they have found, but I can say that my staff is working on it, and they are not trying to find obstacles. They have an affirmative attitude. They are trying to find ways to do this. I am committed to it. and as I say, the Vice President is and our President is. The only thing I can say about the sort of suggestion you made is that the committee ought to consider it, and the staff ought to consider it, and we ought to move as fast as we can.

Senator BAYH. I would like to explore any obstacles or suggestions for overcoming obstacles we can right down to the witching hour on this bill. I know you and the President are committed, and I have said so publicly, and I believe you, to try to move a bill to protect

American citizens wherever they might go. We all recognize the fact that as far as intelligence gathering, the impact that has on American citizens or any other rights that American citizens have, we don't take off our citizenship and leave it when we depart the shores of this country, and to establish a dual standard really concerns me. I am not unaware of the legislative complexities, the difficult nature of resolving these problems, but the concern I have is also a legislative one.

As well-intentioned as you are and the Vice President is and the President is, this bill has been like trying to run in sorghum molasses in January. I mean, it is a tough, difficult, straining kind of job, or more important, and what concerns me is that once we have given birth to this bill, and it is statutory on the books, I wonder if we might not have run out of gas as far as the ability to move any kind of legislation. In other words, we have a great deal here to deal with the problem at home. We understand it is more important. It affects more Americans than those abroad, and once we have discharged that responsibility, I wonder how many of our colleagues and how many citizens will have said, well, they have done enough already.

Attorney General BELL. There is a decision here in the District of Columbia by district Judge Jones involving Americans overseas. Once we enacted this legislation, we could make a respectable argument to a court that if you wanted to surveil an American overseas we could go to one of the seven judges and get an order, the same as we would on an American in this country. If we can build on this one court decision, it is possible that the apparatus of this bill might cover Americans overseas.

We don't know that now. I started out thinking that we ought to extend this bill to Americans overseas. I viewed it as a simple thing but people who are experienced think it is not simple. I don't know. If we go ahead and pass this, we would commit to try to use this bill as a vehicle for getting orders covering surveillance of American citizens overseas.

A lot of times you can get a statute and build on it by court decision. In fact, a lot of people probably object to that sometimes. It goes beyond filling the interstices, as Cardoz calls it. Some people say the court just changes laws or statutes. I think this would be maybe in the nature of filling in interstices, if we could ask one of these seven judges to issue orders on overseas surveillance. I would try that. That might simplify it if we could do that.

Senator BAYH. If a case like that were to arise, would you be prepared to have the Justice Department argue on the side of extending the provisions of this act to cover American citizens abroad?

Attorney General BELL. I would. We took that position on some matter the other day that might involve something overseas, and the same district court decision. Before that decision was rendered, it was not thought possible to get a court order in such circumstances, because there is no statutory method for such a thing. Now, through this bill we are going to build in a court procedure. We would commit to try to do this with respect to overseas surveillance and it might solve the problem.

Senator BAYH. Well, that commitment rests easier than no commitment. Let me say in all respect I think we all understand that is more

to the chance or the whim, if you please, or the good judgment of a given judge at a given time in the future, and it is not as certain as trying to get it in this particular legislation. Let me ask you——

Attorney General BELL. I am not trying to keep you from going ahead with your own thoughts.

Senator BAYH. I understand.

Attorney General BELL. I am just telling you what we might be able to do.

Senator BAYH. It is comforting to know that you would be prepared to do that. Let me look at two types of problems that you refer to in your statement to see if there is perhaps room in which we can at least move into this area to some extent with your support. The first is that the surveillance abroad, of course, often if not always has to be done with the cooperation or involve the cooperation of foreign police and intelligence services, and the second is that there must be different targeting standards for Americans abroad.

Now, as I read the bill, a requirement for minimization procedures, to limit the use of information, that is one of the things we are concerned about, how information found abroad or anything else is used as it relates to Americans, whether they are targeted or not. I don't think the minimization, which is a critical thing, would be affected by these problems. The requirement applies to the use of information by the U.S. Government. It does not make any difference who is targeted, or it seems to me it could be structured in such a way it doesn't make any difference where the information is picked up.

In other words, would it cause any problem to add a requirement in the minimization section that minimization procedures be followed for handling any information acquired abroad about U.S. persons? In other words, when our Government gets the information, whether it is acquired or that citizen is abroad or at home, as far as the minimization, having those machines or having our system automatically throw into the wastebasket information about citizens that don't meet a certain standard, couldn't that be applied to citizens while they are abroad, information that is collected abroad?

Attorney General BELL. Well, I would have to say that is half a loaf. If we go that far, then you have just got one more step to apply to Americans overseas, to put them under this bill: the minimization procedures. Now, if it is up to me to put them in, the Attorney General, I will do it. I have no objection to telling me to do it. Who else would do it? Would it be some judge? Would we go to some American judge, one of these seven, and say, we are getting ready to surveil somebody in West Berlin, and we want you to approve minimization?

If we are going to do that, we might as well say, well, what about an order? So, I don't know that that fits in well. If the Attorney General is to be charged with that duty, it suits me fine, because we do that now, and maybe we should be on a statutory injunction to do it.

Senator BAYH. Well, that could be a temporary, at least certainly a better step than having nothing there at all, it seems to me, because the collection of information per se is not what is dangerous, but what is dangerous is the philosophy expressed by a colleague from North Carolina in quoting Justice Stone that sort of on the present they are waiting, and that information can come back to haunt you later on.

Attorney General BELL. Well, I think you might charge the Attorney General, whoever the Attorney General might be. I think that would be a great improvement over what Chief Justice Stone did. Senator Morgan was talking about Stone. It is too bad Stone didn't do something to insure his words. We never had any statutes. You know, he selected J. Edgar Hoover as head of the FBI, and I have been looking since I arrived in Washington for some charter or statutory authority on domestic security matters. I don't object to statutory commands or injunctions. I think that the FBI does not object. So if you want to put that in the legislation, it would be fine with us.

Senator BAYH. Thank you, sir. What about the targeting, the other part of this particular problem where this has to be done, and oftentimes is done, anyhow, with the cooperation of foreign governments. Couldn't we establish certain standards, legally enforceable standards, so that when we were cooperating with a foreign government, they would understand what standards we intended to be applied to American citizens if they were targeting on them?

Attorney General BELL. That is a problem. How can we tell a foreign government that they have got to get under our standard? Maybe we are just cooperating. Maybe we are just going along with foreign police.

Senator BAYH. Let me tell you how. Let me just give you a specific example which I think we both know is probably the rule rather than the exception. Mr. X, a citizen of the United States, suspected of being involved in clandestine activities with a foreign power, operating abroad, would not be applied in this country, might not be applicable under this standard. We don't have the capacity to bug Mr. X's telephones, so we go to the German secret police, or the police in Bonn, and ask them to do it for us.

Now, it seems to me that if we ask a foreign power to do something like that for us, we also can suggest what the standards are to be applied before they do it, can we not?

Attorney General BELL. Right. That is an easy case. Now, let's take a hard case, one where the Foreign Intelligence service is going to surveil anyway.

Senator BAYH. But do you have any objection to that particular?

Attorney General BELL. No, not the first one, not the one you posed. But the Foreign Service they might be preparing to surveil an American citizen anyway, and they tell us they are going to do it. We can't stop them, and yet we know about it. We are tainted. That can happen. Or there can be one where you are just working a case together, and maybe in that middle ground you can get an American court order. It would take a good deal of judgment about this. This is, see, the case I am committed to, where we would go to the judge ourselves, and that would be where our people wanted to do something, but based on what I have learned about, say, the DEA operations overseas, there is a great deal of cooperation with foreign governments, foreign police.

Frederick Baron just handed me a note that we ought to discuss this further in executive session. What we are saying now, of course, is perfectly all right to be talking about here, but we cannot cover

too many details. Sometimes it is necessary to discuss particular cases as examples. Last week I was working with my staff on what to do about some of the FBI domestic security investigations, and we were trying to devise a rule to help guide our thinking, along with Senator Huddleston on charter legislation. I concluded we never would get a good rule until we could run through about 10 or 15 cases, study facts, and we would come up with a rule. We started doing that, and I think this is that sort of a thing. I think we would probably have to talk to our friends in CIA about this.

Senator BAYH. I understand there are some things that we know what the hardships are when we meet the tough case, and what I would like for us to try to do, and here again I just get back to what I said a moment ago, which I guess is a matter of legislative judgment, taking your judgment and our collective judgments and see whether we feel there is going to be enough staying power to pass two bills in the foreign intelligence area. I am very concerned, Mr. Attorney General, that it is going to take all of us, mustering our strength and cooperation, to get one good bill passed, without discharging that responsibility and then having to come back and get what we all understand is a very minor part of the problem compared to the major one of how we conduct intelligence in this country.

Attorney General BELL. I think that is a very good point. It is hard to get a major piece of legislation enacted. We will not take the process lightly. I will be glad to meet with my people again and see if there is any way possible to devise some kind of an amendment here, so that we could argue to an American court that they had authority.

Senator BAYH. I think there is common ground. We will proceed, but I have a number of questions, and I have been watching the clock. I would rather confine my questions so we will have time and then I can come back if I have others.

Our distinguished ranking member, Senator Garn, is here. Do you have questions or comments, Senator Garn?

Senator GARN. Just a brief comment. Mr. Chairman, on this particular point. I am sorry, Mr. Attorney General, I was late, but I only serve on three committees, and all three of them met at 10 o'clock this morning, as usual. That Senate reorganization really helped us, didn't it? But on this particular point of whether this problem of American citizens overseas should be in two bills or incorporated in this area, I do believe we need to address that problem.

You know from our previous conversations that although I am a co-sponsor of this bill, I am not an enthusiastic supported. I think it is a good bill. If I were writing it alone, there would be some things that I would change, but on balance it is sufficient that I could cosponsor it. I do think we run the danger if we try to put too much more into the bill that I could no longer support it, for whatever that is worth. It may not be worth very much, but nevertheless, I would prefer—let's make that statement at this time—to see the problem of Americans abroad handled separately, as we originally talked about doing. That was one of the reasons I decided to support this particular bill since we would address that problem in a separate one. There are trade-offs that are going to have to be decided, we must decide whether to push and incorporate everything into one omnibus bill or not.

Attorney General BELL. The thought I intended to convey was that I did not want to appear recalcitrant, to have a closed mind. If some way on the merits it appeared that we ought to amend the bill, we would certainly consider it. We think it is very much in the public interest to pass this bill. If we can do what Senator Bayh wants, we would certainly look at it.

Senator GARN. Well, I agree with you completely, and I hope you don't misunderstand what I say, because Senator Bayh and I worked on this similar bill last year at great length. It seems like we spent most of the year on it. We saw each other more than we did our wives, which I don't prefer either, but nevertheless——

Senator BAYH. I am glad to hear that.

Senator GARN. We were not able to get it through due to the lateness of the session, and I do think that it is highly important that we do pass a bill, because in the current situation a lot of people seem to forget that there is no law covering this area at all; that the President, whoever he might be, can simply order electronic surveillance if he declares it is in the national security interest, and I think that is wrong. I think we have a good chance of passing this bill by talking to a lot of our colleagues. It is a controversial bill. I am afraid if we try to put too many things into it we lessen the chances of passing it. I understand what Senator Bayh is saying, that on the other hand maybe it lessens the chance of passing the second part. If I have to choose, I would rather take S. 1566 and get it passed—take our chances on the second part—than lose the whole ball game. That is the point that I am trying to make.

Attorney General BELL. I agree with that.

Senator BAYH. Thank you, Senator Garn.

Senator Huddleston?

Senator HUDDLESTON. Thank you, Mr. Chairman.

Mr. Attorney General, one of the great potentials for use from intelligence gathering once you have established the procedure under which electronic surveillance may be conducted is the use of the information that might be gathered in such surveillance, much information that may have no relationship to the original objective or intent for the surveillance, but which if placed in certain hands or used in a certain way could be very damaging to an individual.

Are you satisfied that the so-called minimization procedures established in this bill are adequate to protect the citizen from the misuse of information that may be gathered?

Attorney General BELL. I am. I have had some experience with the subject since I have been here. Of course, the only minimization that we have now is whatever I prescribe.

Senator HUDDLESTON. Right.

Attorney General BELL. I think we would have a double safeguard. We have the Attorney General plus the people in the chain who suggest minimization as it comes up to the Attorney General; and then we also have the court. The court is charged under this bill with imposing minimization standards.

Senator HUDDLESTON. That is correct.

Attorney General BELL. I think that is a very good feature in this bill.

Senator HUDDLESTON. Do you believe that is important?

Attorney General BELL. I think it is very important. We have had too much dissemination. Not even gossip-level dissemination so much as dissemination due to carelessness or without thinking. Who needs this? Who is harmed by it? Those are the two things you need to think about, need and harm, and constitutional rights, privacy. So, I think the American people need the imposition of minimization standards.

Senator HUDDLESTON. Because we uncovered in previous investigations where one agency would take information gathered by another and use for its purposes, although the original purpose of the gathering had no relationship to what the second agency was trying to accomplish, but found that it might be very effective in carrying out some of its objectives and this seems to me to be a real serious danger and a serious problem that we have in the information we gather on our citizens.

The question of congressional oversight, I thought last year's bill was much stronger in giving Congress the oversight that it might need, and in particular this committee. The present bill requires reporting to Congress only the number of applications made for court orders and extensions and the number of orders and extensions granted, modified, or denied, as I understand it. Is there any reason why the bill should not also contain more specific reporting requirements for this committee, so that we can fully discharge our responsibilities under Senate Resolution 400?

Attorney General BELL. I think it would be a mistake to freight the bill with a lot of reporting procedures when we are already reporting. We are negotiating a reporting system with your committee staff right now and I am told it is 12 pages long. We will report anything to you under your Senate resolution to create the committee. It seems to me you are never going to have enough in the statute to cover it anyway, so why do that? Why not just leave it to the normal relationship between us and the committee?

Senator HUDDLESTON. Last year's statute, though, was a little more direct in saying that nothing shall be deemed to limit the authority of the Select Committee on Intelligence to obtain such information as it may need. They left the initiative more or less, I guess, with the committee in determining what it needed and what it could ask for.

Attorney General BELL. Now, we don't have any objection to some general requirement. I am objecting to specifics, and I wouldn't think you would want to inject specifics.

Senator HUDDLESTON. I just don't want any limitations on the committee to ask for whatever it might deem to be necessary to carry out its responsibility.

Attorney General BELL. We don't object to that. Now, when we get to the House side, this could be a problem. You know, we are under seven committees there. They are in the process of creating a committee, but I am not aware of what preemption of jurisdiction is proposed. I hope you will have that in mind.

Senator HUDDLESTON. Well, we certainly will. We understand the problems on the House side, too, although I think maybe they are beginning to move in a more desirable direction. In the past, of course, intelligence agencies have used warrantless physical search techniques,

including surreptitious entry and mail opening, to gather foreign intelligence information in the United States. This bill, of course, does not mention these particular techniques. If Congress does not clearly prohibit them or set standards for them, could they still be used on the basis of inherent Presidential powers?

Attorney General BELL. It could be, but we are working on legislation in that regard also.

Senator HUDDLESTON. You plan to have separate legislation relating to surreptitious entry?

Attorney General BELL. We made a considered judgment that we could not pass all of that in one bill, that we would not get anything. While it may seem strange for me to be indicating that we want to give up power that we now have, we do. We have the same objectives, and we don't think we can pass all that subject matter in one piece of legislation.

Senator HUDDLESTON. So we can expect further legislation on that subject?

Attorney General BELL. Right.

Senator HUDDLESTON. Well, as I pointed out earlier, this is the first piece of charter legislation for the intelligence community, and I am somewhat concerned about the impact on the future charter legislation that, as you know, we have been working on. Would the adoption of a noncriminal standard for electronic surveillance lead to the adoption of similiar standards for other activities such as surreptitious entry or mail opening in future charter legislation?

Attorney General BELL. I have to say that apart from that, under this 2521 (b) (3) (i), that if those same circumstances applied, I would be in favor of using the power of the President to allow entries or searches or whatever is needed. That provision seems to be the subject of a good bit of writing these days, but if you will read that carefully, I think you will have to say that whoever fit into those circumstances ought to be surveiled, and that is pretty near a criminal standard in itself. Maybe you are writing one when you are putting it in this bill, but I have some trouble finding how anybody could argue against that. Now, you can argue about something else off on the periphery somewhere, a general thing, like we ought to always have a criminal standard, but when you read this, that in itself is tantamount to a criminal standard.

So, what I say is, yes, if we found those circumstances I think it would be against the national interest for me not to take note of it.

Senator HUDDLESTON. I just have one other item. The question of the terms of the judges, Senator Morgan used the term leading to the possibility of judge shopping, which I hadn't heard of before, but I guess these fellows that practice law are accustomed to it.

Senator MORGAN. The judge knows what I am talking about.

Senator HUDDLESTON. I am sure the Attorney General knows what he is talking about. Do you see anything wrong with setting terms perhaps for these judges? As the bill is written now, I understand there are no terms, so that they would be reappointed from time to time. They would be serving on a staggered term basis of a given number of years each?

Attorney General BELL. No, no, I really hadn't thought about that until this morning, and I must say that I favor terms. I would favor that amendment. I think it would be bad to put judges on the panel and leave them there forever.

Senator HUDDLESTON. There ought to be some procedure to replace them or to at least have to consider it.

Attorney General BELL. This idea of somebody having a 7-year term—staggered to replace one every year—wouldn't be a bad approach to it. I might as well speak to the judge shopping because there are 415 Federal District judges, and we are only putting seven in the bill. There is a judge shopping in the sense that you could go to any one of those seven. Whereas if you had a venue requirement, you might have to go somewhere where there is only one. Of course there are very few districts left now where there is only one judge, so I don't think there is that much of a problem. We had one not long ago where we got a lot of title III's, as you know, and sometimes those are in places where they have 25 judges, sometimes maybe they have one or two judges. We have to go to the district where the wiretap is going to take place.

I think seven is a reasonable approach to it, but I do favor some definite terms. I had not thought about that. I just had it in my mind that probably the Chief Justice would rotate them, but it would probably be better to specify.

Senator HUDDLESTON. Specify it in the legislation?

Attorney General BELL. I think the more specification we have, the better off we are.

Senator HUDDLESTON. Thank you, sir. Thank you, Mr. Chairman.

Senator BAYH. Senator Chafee?

Senator CHAFEE. I have no questions, Mr. Chairman.

Senator BAYH. Thank you. Senator Morgan?

Senator MORGAN. Judge, could you tell me, you stated earlier that you thought it would be in the public interest that we pass this legislation. Could you tell me what you consider to be the difference between the law as it is now and what it will be under this legislation, with regard to electronic surveillance of Americans?

Attorney General BELL. The difference will be the use of a judge who will be superimposed on the chain of command above me, above the Attorney General. I perceive that to be in the public interest, because the American people trust courts. Even if they didn't trust courts as much as they do, they would feel better if there were someone else in the chain of command. Even if we added the chairman of this committee to the chain of command, that would bolster the confidence of the people in the system. I think the system, based on what I know about it—during this administration—the system works well as it is, and there are no abuses taking place. It is important nonetheless for the American people to have confidence in the system of government, and this is nowhere more true than in an area where there is some secrecy involved.

So, that is why I say it is in the public interest. That is why I am pushing this. I am not worried about anybody losing their rights now.

Senator MORGAN. Judge, what do you consider to be your authority? What do you consider to be your authority now to engage in electronic surveillance of an American under the present law?

Attorney General BELL. Of an American citizen?

Senator MORGAN. Yes, as Attorney General.

Attorney General BELL. I have none whatsoever. I have not surveiled an American citizen.

Senator MORGAN. Do you consider that anyone, including the President, has the inherent right to engage in electronic surveillance of an American citizen in this country?

Attorney General BELL. I do. I think he has a constitutional right to do that, and he has a concomitant constitutional duty to do it under certain circumstances. I have said in the confirmation hearings that I would not do it on my own. I believe those were the words I used, "on my own."

Senator MORGAN. I assume you base that on the national security aspect.

Attorney General BELL. Foreign intelligence. What is it? What is the exact language in the Constitution? Foreign policy powers.

Senator MORGAN. Judge, do you have a brief on what you consider to be the inherent powers of the President with regard to electronic surveillance that might be available to this committee?

Attorney General BELL. We don't know of one offhand but we would be glad to prepare one for you.

Senator MORGAN. I think it would be interesting, because I have some difference with regard to what I conceive to be the President's right in this connection.

Attorney General BELL. We would be glad to try to support that by brief if you would like to have us do so.

Senator MORGAN. All right, sir. Now, in this bill I understand that, of course, to get a warrant to engage in surveillance you have to have a certification. Is that from the President or the Attorney General?

[The material referred to follows:]

SEPTEMBER 2, 1977.

Hon. ROBERT MORGAN,
U.S. Senate,
Washington, D.C.

DEAR SENATOR MORGAN: During my testimony concerning S. 1566, you asked if the Department of Justice could provide you with a statement outlining the basis for the Department's conclusion that the President may approve warrantless electronic surveillance in the United States under certain circumstances.

In every case in which the issue has been directly raised, the decision has been that the President may lawfully approve warrantless electronic surveillances of foreign powers and their agents. *See United States* v. *Buck*, 548 F.2d 871 (9th Cir. 1977); *United States* v. *Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc); *United States* v. *Brown*, 484 F.2d 418 (5th Cir. 1973); *United States* v. *Clay*, 430 F.2d 165 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971); *United States* v. *Enten*, 388 F. Supp. 97 (D.D.C. 1971), *aff'd in part and vacated in part sub nom., United States* v. *Lemonakis*, 485 F.2d 941 (D.C. Cir. 1973); *United States* v. *Hoffman*, 334 F. Supp. 504 (D.D.C. 1971). In *Buck*, the most recent case, the Ninth Circuit referred to such warrantless surveillances as a "recognized exception to the general warrant requirement." The Supreme Court has not addressed the question, but has taken pains to make clear that its decisions requiring warrants in other circumstances do not apply to surveillances involving foreign powers or their agents. *See Katz* v. *United States*, 389 U.S. 347, 358 n.23 (1967); *United States* v. *United States District Court*, 407 U.S. 297, 308, 322 & n.20 (1972).

In *Butenko*, the opinion which undertook the most substantial analysis of the issues involved, the Third Circuit initially determined that the President had as incident to his Article II powers the power to gather foreign intelligence

information. 494 F.2d at 601, 603. The court then determined that this power could be exercised only in accordance with the Fourth Amendment. 494 F.2d at 603. The court recognized that the Fourth Amendment bars only unreasonable searches but acknowledged that a prior warrant is the normal test of whether a search is reasonable. Referring to other exceptions to the warrant requirement, however, the court weighed the costs of requiring a warrant against its benefits and determined that because of the need for secrecy and speed in foreign intelligence surveillances and the opportunity for occasional post-surveillance review, a warrant was not required. 494 F.2d at 605. The court made clear that this exception only applies where the primary purpose of a surveillance is to gather foreign intelligence. 494 F.2d at 606.

The holding of the District of Columbia Circuit in *Zweibon* v. *Mitchell*, 516 F.2d 594 (1975) (en banc), is not inconsistent with *Brown* and *Butenko*. In *Zweibon* the court held that a prior judicial warrant was required for electronic surveillance of persons who were neither agents of nor collaborators with a foreign power. While in dictum a plurality of the court suggested that a warrant should be required even where the subject of the surveillance was an agent of a foreign power, the court made clear that its actual decision was not so broad.

In light of this case law and in the absence of statute, the Department of Justice has consistently maintained that reasonable surveillances conducted against foreign powers and their agents, personally authorized by the Attorney General pursuant to an express Presidential delegation of power, are lawful absent a warrant.

Yours sincerely,

GRIFFIN B. BELL,
Attorney General.

Attorney General BELL. Attorney General.

Senator MORGAN. And it is proposed——

Attorney General BELL. The Assistant to the President in charge of the National Security Council would certify to me.

Senator MORGAN. And then certify to you?

Attorney General BELL. I certify to the court.

Senator MORGAN. Now, you can delegate that authority to an Assistant Attorney General?

Attorney General BELL. Well, I put that in the bill thinking it would be a good thing, but in the Judiciary Committee there seemed to be some objection to it. I don't know if that is going to survive or not. I was hoping it would. I spend a lot of time on these matters, and the question is one of judgment. Does the Congress want the Attorney General personally to do it or would it be satisfied to have an Assistant do it with the Attorney General? I do that in title III, wiretap. I delegated that to Mr. Civiletti, head of the Criminal Division, but he gives me a weekly report on what he has done, and I see that every week. That is the way I handle this, and I also told the Judiciary Committee that I would agree to do it for a certain length of time to get it running right, to get the safeguards in it and the kinks out of it before I delegate it.

Senator MORGAN. Well, Judge, I might say I think it is a two-edged sword. I fear that delegation of the power to an Assistant Attorney General, if it is done routinely or laxidasical, and yet on the other hand, knowing the demands upon the office of Attorney General, I am afraid that the Attorney General might be put in a position where he had to routinely approve someone else's recommendations, and so it might be better to give it to an Assistant, provided this Assistant has had powers specifically confirmed or considered in his confirmation hearings.

Attorney General BELL. That is a good point. I ought not to be allowed to select any Assistant. I think the Assistant, if he is going to be delegated, ought to be known. You ought to know that when you confirm him.

Senator MORGAN. Quite frankly, I think I would be better satisfied with one who was confirmed knowing that that was going to be a part of his responsibility than I would be saying that the Attorney General himself had to do it, knowing of all the responsibilities that you have, because you would have to do it routinely upon what somebody put before you.

Attorney General BELL. I think that is a very good point. Nobody made that point before.

Senator MORGAN. Let me go a little further. Now, if this certification had come from the President's adviser, as I understood the bill, last year the judge couldn't look back of a certification. Now, it is not quite clear to me how far the judge can look back of it this time. Can he go back into the facts on which the President's adviser made the certification, or is he limited solely to the facts certified?

Attorney General BELL. He can examine the facts and he uses a clearly erroneous standard in making his decision, and he can ask for additional facts. In other words, we go down to Judge *X*, and he says, I don't know about this, give me some facts.

This is my present practice. I tell the Bureau to bring me some more facts on this if I am not satisfied with it. Sometimes I turn them down without asking for additional facts, but that is what the judge could do, and that is new in the bill. I don't think you ought to ask a judge to rubber stamp things, and I don't think you ought to restrict him so that he has to say yes or no.

Senator MORGAN. I don't think any real judge would even want to carry out responsibilities of issuing a warrant if he could not look at the facts, but it is not quite clear to me from the bill that he can go behind those facts. I notice that Frederick—I wonder if Frederick has the section there.

Attorney General BELL. Yes; here it is right here. "C: 'The judge may require the applicant to furnish such other information as may be necessary to make a determination required by section 2525 of this chapter."

Senator MORGAN. What page is that?

Mr. BARON. Page 15 of the Judiciary Committee print for July 18, section 2524.

Attorney General BELL. And then the standard is on page 16. On 15, he can get some more information, and then he is tested over on 16 by the clearly erroneous standard.

Senator MORGAN. The thing I am still not quite clear on, I think from what you say the judge may be able to go back to the facts on which the President's advisor based his certification, but are we sure of that fact?

Attorney General BELL. Well, this is broad language. That is the way I would construe it, and I would get the facts for a judge, if any one of these seven judges wanted some more facts. Now, if, we will say, the chairman, or the assistant for national security were to say, well, we can't give those facts out, I would say, that is the end of the deal,

then, and we can't get the order, so forget the whole thing. I can see how you would run into something like that. The judge doesn't have to grant the order. He has the upper hand. He has the final say.

Senator MORGAN. Mr. Attorney General, I am satisfied, knowing you, that you would do exactly that, and I am also satisfied, knowing this administration, that they would do exactly that, but it kind of worries me, looking down the road, as to who might be occupying your position or who might be occupying the White House.

Attorney General BELL. Well, you might want to doctor that language some and make it a little more explicit. There would be nothing wrong with that, because that is our intention, that this judge have the authority to get information on which to make a judgment.

Senator MORGAN. Well, my time is a little close. I will make a note of that and get with some of your staff and maybe we will talk some on that. With regard to the term of judges, you have no objection to some rotation system?

Attorney General BELL. Not at all.

Senator MORGAN. Now, is it your idea or your understanding, Judge, that these seven judges would be located in the District of Columbia, or would they be around the country?

Attorney General BELL. Well, they ought to be in the environs of Washington, but I don't think they all ought to be in the District of Columbia. I think the American people think that there it too much power already vested in Washington. At least that is what the ones tell me that I have talked to, and I think they might feel better if we had some judges in Maryland and Virginia that it wouldn't take a day's travel to get to.

Senator MORGAN. I certainly would agree with that. With regard to my thought on judge shopping—and I started to say I didn't mean this to reflect one way or the other, it is just that I will make the statement. It is a fact that——

Attorney General BELL. Well, you and I both practice law. We know it is a lawyer's practice.

Senator MORGAN. And what bothers me is, if these seven—to give you an illustration, there is a judge in my home capital that absolutely will restrain the State of North Carolina—a State judge from doing anything, and the lawyers knew this, and they knew that any time they wanted to restrain an act of any kind of regulatory board or the commissioner of revenue, that this judge would restrain them, and also in my State we had a judge that would restrain law enforcement officers from doing anything just on any preliminary showing.

As a result, lawyers seeking injunctions shopped for these judges. Now, how are we going to prevent this from happening with these seven judges?

Attorney General BELL. I will tell you exactly how to do it. Put in one of your staff reporting requirements a requirement that we report on the names of judges and the number of petitions presented to particular judges. Then you will be able to see that we are using one judge more than all the others. You can see that in some types of cases in the Justice Department in years gone by, where they shopped. You will pick that up and you will make us do something about it.

Senator MORGAN. What can we do about it? That is an interesting thought.

Attorney General BELL. You can simply call the Attorney General over here and tell him, I believe you are abusing your authority.

Senator MORGAN. Would someone then have a right to designate another judge? Do you think maybe we ought to preserve that right for the Chief Justice or the Attorney General to change? It may be you have a judge that just won't ever grant any, and it might be the other way.

Attorney General BELL. That is right, it could be the other way.

Senator MORGAN. It seems to me we might want to put some kind of a saving clause in there, too.

Attorney General BELL. Would you think that we could agree that the judge would serve at the pleasure of the Chief Justice and for no longer than 7 years?

Senator MORGAN. It would suit me better, because I think the Attorney General and this committee and the Congress——

Attorney General BELL. Also, you could have a judge that might become senile or become an invalid, have a stroke or something, so you need some way that you could change the judges.

Senator MORGAN. Without having to wait for the 7.

Attorney General BELL. For the 7 years to run. I think at the pleasure of the Chief Justice would be a good proposal for it.

Senator MORGAN. Judge, one other question. I fear I am encroaching on someone else's time. Suppose, as I understand the standards, and I don't have them before me, but as I understand it, if the advisor to the President has reason to believe that I as an American citizen may be passing information to a foreign government, can they go in and get an order for electronic surveillance without specifying the kind of information they think I might be passing, and how far beyond mere suspicion do they have to go?

Attorney General BELL. Well, there has to be probable cause. We use a probable cause standard, and we now have something along that line going, and have had in the past, where we used title III, which depends on what sort of a crime was involved. So it is not unheard of to do this now in title III. This facilitates it. Sometimes you have something that is in foreign intelligence, and it fits into a criminal statute also and you can function under title III, but not very often.

In the warrant application, we have to put in the facts as to the type of information sought to be acquired, and when the target is a foreign power, the designation of the type of foreign intelligence and nature sought to be acquired. What the judge wants to know are the facts on which you could ascertain probable cause. Now, we have got a certificate that is like an affidavit, when you get a warrant. The certificate would contain the facts. When I certify now, they give me—the FBI sends me over something, sometimes three pages, sometimes maybe seven or eight pages, and it gives all the facts, as tantamount to what you do when you go before a magistrate to get a warrant, a search warrant.

Senator MORGAN. Judge, would you certify now, and maybe this is too direct, but I will ask it: Would you make a certification which would entitle an agency to surveillance for the person who is accused of passing information which in your opinion would not constitute a crime, such as espionage? I understand the law does not require that, but what I am talking about is, as a matter of practice, would you now permit

surveillance on an American citizen just on the information that I might be passing information to a foreign power, even if you knew that I was doing it, and if that information—if I was passing it, it still would not constitute a crime?

Attorney General BELL. Well, that is a hard question. You have got to know what the information is, and under the espionage law, as I understand it, they restrict it to defense material, and some of this is not defense material. Some are documents that have something to do with the State Department, with diplomatic matters, or they might just be technological information that could be either way, and that would get down to what you asked me, what would I do about it.

You would have to give me a case. I could give you a case or two in executive session.

Senator MORGAN. Suppose we are talking about, I am passing computer technology to one of the Soviet nations, which could be helpful and might be helpful to them in many ways. Would not national defense, couldn't that have a broad—wouldn't it have a broad enough interpretation to let us use the criminal threshold, and if it does not, couldn't we broaden it easily enough to satisfy some of the questions that some of us have or the fears we have?

Attorney General BELL. Well, Judge Hand gave an expanded interpretation of national defense in *Gorin* v. *United States*, 1941. Judge Hand who, as you know, was a judge of some note, said he construed it narrowly. Now, we who are worried about the security of the Nation, we haven't got time to worry about every judge in the country deciding whether it is going to be narrow or broad.

Senator MORGAN. Well, couldn't we in this Congress, in this bill, broaden it? Of course, I think we would have to all acknowledge that since Learned Hand wrote that opinion the courts have been more inclined to construe things liberally, but what I am trying to say, and I am not trying to argue, but I am trying to say, can't we make the criminal threshold——

Attorney General BELL. Here is what I would like for the committee to do. You have been an Attorney General, and you understand statutory construction. I would like for you to look at this provision we have, this so-called noncriminal standard everybody wants to attack. Four, under (3) (i), page 4. It seems to me that is as near to a criminal standard as it can be. It is like a crime, where all the specifics are set out.

Senator BAYH. If the Senator will yield, I came very close. We put most of that definition together last year, as you know, and it was to try to get at the deep concern that many of us had about departing from the criminal standard. We are talking about somebody acting under the direction of a foreign intelligence mechanism, agency, on the payroll of some foreign intelligence gathering. They are directing or acting in a manner that is clandestine, where information that is being passed could damage the country. I share the Senator from North Carolina's concern, but I guess—and I apologize for interrupting here, because I know you are just about through, but the one legitimate area where it seemed to me that perhaps intelligence people had a leg to stand on that normally I wouldn't think they would is

in that area where you just don't know exactly what kind of information is being passed, but you have every reason to believe, and you know this person is acting under the direction of a foreign intelligence gathering or foreign intelligence agency. Then maybe that exception could be——

Attorney General BELL. If you put a parenthesis here and said, "This section constitutes a crime," parenthesis closed, this would end all this argument. That is all it is.

Senator MORGAN. Well, you know, that may be what I am trying to say, because it worries me that we are going to open a door.

Attorney General BELL. If I see many more editorial columns, I may put that parenthesis in there. [Laughter.]

Senator MORGAN. Thank you, Mr. Attorney General. Thank you, Mr. Chairman. I apologize for exceeding my time, but I will talk with Mr. Harmon and Mr. Baron.

Attorney General BELL. By the way, we will be glad to answer any questions in writing if any member has a question they want to submit to us.

Senator BAYH. I just want to read this. You know it and all of us know it, but some of us may not have had the latest version of the noncriminal "crime" standard. "Pursuant to the direction of an intelligence service or intelligence network of a foreign power"—that is the way this American citizen is being prompted or acted—"knowingly collects or transmits information or material to an intelligence service or intelligence network of a foreign power"—so there you have that nexus—"in a manner intended to conceal the nature of such information"—that is where you have the problem; if you knew what kind of information it was, you could nail them dead center, but you don't quite know, but you have every reason to believe, because of the nature—"such information and material, the manner in which it is concealed, or the fact of such transmission or collection under circumstances which indicate the transmission of such information or material would be harmful to the security of the United States, or that lack of knowledge by the United States of such collection or transmission would be harmful to the security of the United States," and that comes as close as you can come, I think, but I guess we would all rest easier if it came there.

Senator MORGAN. Well, how close does it come?

Attorney General BELL. I think it is a crime myself.

Senator MORGAN. I would agree with you.

Attorney General BELL. But we haven't called it that. It is like giving a dog another name.

Senator MORGAN. Mr. Chairman, could I pursue one other question? And I am way over my time. Judge, the next provision that bothers me is the conspiracy thing. Having tried a few liquor cases in the Federal Court, where my clients got hooked right easily when one act had been caught, does that encompass all of the broad rules of conspiracy that you and I——

Attorney General BELL. It is as broad as the Federal law of conspiracy.

Senator MORGAN. Then it is pretty broad.

Attorney General BELL. It is pretty broad, but we never have felt sorry for any of our bootleggers before.

Senator MORGAN. Well, I have been on the other side.

Attorney General BELL. I wouldn't worry too much about the spies if we are not going to worry about the bootleggers. Many lawyers and lay people, as you know, object to the breadth of the Federal conspiracy law.

Senator MORGAN. In all seriousness, it is a broad law, and when we look at this new criminal code bill I hope we will look at the conspiracy, because I do feel like there have been times when injustices have been done to individuals because of the broadness. Once you establish an act, then you can bring anybody under the sun, but we will talk about that later.

Attorney General BELL. All right.

Senator BAYH. Well, just for the record, Mr. Attorney General, one of the concerns I have, and I think the Senator from North Carolina and others have, is the interpretation of this standard not being nailed down the way I think most of us feel it ought to be, and I think we have reason to believe it is with this language. If we are talking about a citizen here, a citizen of the United States who is on a first name basis with the ambassador of another power in this country, the ambassador or somebody in the agency or in the embassy who might indeed be on one of the foreign government's intelligence agencies, and let's say it is a traditional kind of ethnic problem or ethnic concern that many of our citizens have, if that embassy person or if the ambassador asks the American national that particular country's American nationality, I mean, Greek American, you can name it, there could be half a dozen where there would be important issues, and that citizen then talks to somebody in Congress or to the President, urges them to pursue a given policy, would you feel that that would apply?

In other words, the normal kind of citizen lobbying that we all recognize as an important right of the citizen. If it has a relationship that might exist as far as some people are concerned and involving an official of another government, would that then fall in this category?

Attorney General BELL. You mean, on conspiracy?

Senator BAYH. Yes, sir. Under the definition right here of subsection III, the noncriminal standard, would that be enough for you to tap that person?

Attorney General BELL. No, I don't think so. I can't believe that it would be.

Senator BAYH. I can't either, but you are the Attorney General, and this is important, sir.

Attorney General BELL. If you go to some embassy and get under their direction, and they tell you, now we are engaged in intelligence work, and we want you to do this and we want you to conceal it while you are doing it, and what you are doing is something that might be harmful to the security of the United States, then you would be guilty. But you are not going to do all those things. You are not going to first act under the direction of a foreign government. If you acted under the direction, to write a letter, to engage in public relations, we'll say, or something like that, you wouldn't conceal the nature of what you were doing, and then second, you wouldn't do anything if it was harmful to the security of the Nation.

Now, if some American citizen wants to do those things, then I would say we would have to go do something to him. It would not be a crime. Apparently we are not going to make that a crime, except in the sense we are going to allow him to be surveiled.

Senator BAYH. Well, now, do we not have one important factor? I mean, I think the fact that the normal kinds of petitions that you get from citizens of the United States to help us in Cyprus, help the Greeks, help the Turks, help the Israelis, help the Arabs. I mean, you know, you can go right down the pecking list of deep concerns that Americans with roots in other countries have.

Attorney General BELL. Let me give you an answer that I believe is better than anything I have thought of. Under the Foreign Agents Registration Act, we would not be able to surveil under that act unless there was also clandestine intelligence gathering. So what you are describing is not clandestine, and we have plenty of Americans registered as foreign agents. We handle that in the Justice Department, and we don't consider that to be a clandestine intelligence activity.

Senator BAYH. Even if it were clandestine, could it be—I mean, certainly the relationship between the goverment in question and the American citizen could be clandestine, but we have the collection and transmission. I mean, the statute says right here, you have to collect and transmit. Just writing to Congress or talking to your favorite Senator and saying, listen, we need more money for *X* and *Y*, that does not conform to the definition as I see it, but I want us to make sure that our legislative record is absolutely clear here.

Attorney General BELL. It is clear. There is no idea of anything like that, and it is not an idea, it is what the statute says. It ties it down.

Senator BAYH. All right. Now, may I ask you to—I would like for you to clarify a couple of other points that might perhaps be made a little bit better here. The way I understand it, the current procedures now where you have surveillance requires high level Executive branch review, including the Attorney General, in, what, every 90 days?

Attorney General BELL. Ninety days.

Senator BAYH. And this one goes on a year in this bill now. Why is it that shouldn't sort of shorten that length of time for review?

Attorney General BELL. Well, we think it is a fair trade-off when you are using a judge, and the 1 year only applies to a foreign establishment. A year is a reasonable time. You don't want to go back to the judge every 90 days on that sort of a surveillance.

Senator BAYH. Would it be too much to go back to the Attorney General every 90 days?

Attorney General BELL. No; I spend a lot of my time now reviewing matters I reviewed 3 months ago. According to what the activity is; we put the 1-year activity in the category that did not seem to us to need reviewing every 90 days, but that is the sort of thing I wouldn't want to say too much about here now, outside an executive session.

Senator BAYH. If we are talking about a narrowly defined foreign power, I would not be as concerned as I frankly am about the fact. I think the bill broadly interprets foreign power. We are talking about directed and controlled by a foreign government. There is no requirement here that the group be engaged in clandestine intelligence activities, sabotage or terrorism, and I am concerned that we not have a back door means to surveil American citizens.

For example, suppose you have an airline that is run by a foreign power.

Attorney General BELL. An airline?

Senator BAYH. An airline, and some of the business activities in which you have at least a few, maybe several agents of the foreign power's intelligence machinery. You also have a number of Americans, particularly if it is a commercial enterprise, and we know the Russians have this one operation out here that is just a front, but there are a number of substantial commercial enterprises, legitimate commercial enterprises that are part of a foreign government, yet you have a lot of American citizens working in that government, in that government-owned enterprise. Now, I am concerned that we not provide a back door means of lowering the standards as far as the protection that these American citizens get. Do you have any thoughts on that?

Attorney General BELL. Well, I frankly hadn't thought of a foreign airline. I think in terms of embassies and trading offices and that sort of thing, where everybody there is from the foreign country, and I hadn't thought of an airline. I don't object to protecting something like an airline that is flying between some other country and this country. That just shows what the human mind can do and why it is good to have hearings.

Senator BAYH. Well, let's give some thought to that in the bill. I would like for you and your staff to give some specific attention there. I am not particularly happy with what we have done there, but as I recall, we have in the language of the bill specified that the surveillance has to be directed at the corporate officials involved, and as near as we can to confine that to those who are involved in the intelligence activity, but still I think we need to look carefully at how we can minimize the potential of sweeping in an American who might be using that phone, and in the event we do, make sure that we crank out any information and minimize that out of the process.

Attorney General BELL. We could in the minimization procedure put in restrictions. That might not be the whole answer, but that might be part of it. I think that since you have raised the point that might be something our staffs ought to look at.

Senator BAYH. Well, let's look at that. To move on here, we have done a lot of discussing about the criminal standard, and we are all a little nervous about that. One of the things that makes me nervous is the fact that we use the phrase there, in the criminal standard, not the non-criminal standard, but if we look at the criminal standard, we use the phrase, "will involve"—in quotes—"will involve a criminal violation." There is no requirement that the violation is about to occur or that it will soon occur, and I wonder, would there be any problem as far as the Government is concerned and those who must perform this mission, if we either limited the standard or set about requiring that the crime will soon be committed or is about to be committed, or tighten it up.

Attorney General BELL. I hope you won't take it out, because that is the very point that is going to come up in the FBI charter on domestic matters. Are we limited to a crime that has already been committed, or can we take note of something that is about to happen? That is a very close question. In the FBI, we are subject to whatever

Congress tells us to do, and if the American people want to restrict the FBI to crimes that have already happened, we would accept that.

Senator BAYH. Well, that's not what I'm saying, sir. Let me try to be more specific here. It seems to me if we say "will involve," that is sort of some nebulous time length there that could reasonably be interpreted to be will involve crime maybe 10 years from now.

Attorney General BELL. Yes.

Senator BAYH. But if we use some of the words of art that are used in other criminal statutes, reason to believe a crime is about to be committed, or will soon occur, to just narrow down the time frame so you're not going on a fishing expedition, but you have reason to believe in the near future.

Attorney General BELL. We'll look at that. I see what you mean. You want to restrict it time-wise. Or, you think it is too open-ended.

Senator BAYH. Yes, I think if you look at those words, it doesn't really say in 10 days or 30 days, but you're really forcing all of us to focus on the fact that well, all right, this isn't something that just may happen out here in 30 days or 30 years, maybe, because it happened once before, but that all the evidence we have indicates that there's something about to happen out there, will soon happen, that it really is close to the kind of crimes, because we're talking here in this area about a crime.

Attorney General BELL. All right, we'll look at that.

Senator BAYH. Let me yield to my colleague from Maine who I see is here now. We appreciate your being here.

Senator HATHAWAY. Thank you, very much, Mr. Chairman.

Before I ask my questions, I want to commend the subcommittee chairman and the Attorney General for their hard work and their dedication which has given us the very complicated bill that we have before us that we may need to take a post graduate course at MIT to thoroughly understand.

I am working on a simplification, General. I hope to run it by you when I'm finished if I ever finish it, just to make it easier for myself.

There are two areas I'd like to question you on. One is in regard to a situation I thought the chairman was going to allude to where you have say, a Canadian or someone from some obviously friendly country visiting here, representing some "foreign power." Are we going to allow surveillance in cases like that, or should we think about narrowing the scope of foreign powers to those countries that we now consider to be adversaries, and therefore not run the risk of wiretapping our friends and creating a great deal of alienation between our country and countries that are friendly to us?

Attorney General BELL. Well, I think perhaps the State Department might answer that better than I, but the point is we are not just going around tapping our friends willy-nilly. They are engaged in clandestine intelligence activities to begin with.

Senator HATHAWAY. I don't think it is a foreign power that has to be clandestine, does it?

Attorney General BELL. Agent of a foreign power.

Senator HATHAWAY. But can't we just tap them for foreign intelligence information or purposes. I forget where that is—what section.

Attorney General BELL. My staff tells me that I am getting in deep water, that I ought to leave this to the State Department and other

intelligence agencies, without speaking for them. So I think I had better take the advice of my staff.

Senator HATHAWAY. Because if you take, first of all, on page 2, "foreign power" means a foreign government, which would include Canada. And then "Foreign intelligence information" on page 5 means information to conduct the successful conduct of foreign affairs. So it could mean that we could tap some——

Attorney General BELL. Yes.

Senator HATHAWAY [*continuing*]. Emissary or visitor from Canada if we had reason to believe they were connected with some company or connected with the government and could give us some information to help us conduct, say, our fishing boundaries negotiations that we are now engaged in, or minerals or whatnot.

[Pause.]

Attorney General BELL. I had always thought that the foreign friend that you were speaking of, to be surveilled on page 3, would have to be an "officer or employee of a foreign power." Now you may object to that—or he "knowingly engages in clandestine intelligence activities for or on behalf of a foreign power."

Senator HATHAWAY. Yes, but those are in the alternatives, right?

Attorney General BELL. Yes, "or".

Senator HATHAWAY. So if he is an officer or employee of a foreign power, he could be an officer of a Canadian bank or an airline.

Attorney General BELL. That's the way I understand it.

On that part of it I think you ought to ask the State Department or the CIA witnesses.

Senator HATHAWAY. We ought to have them testify.

Attorney General BELL. They are going to testify and they can tell you the reason for that.

Senator HATHAWAY. You wouldn't care if we eliminated that, or if we just restricted this to adversaries. Eliminated friendly countries.

Attorney General BELL. Well, I couldn't agree to that right now without thinking about it. I see a lot of countries, and there are shades of countries. You're on a relative basis when you talk about "friends."

Senator HATHAWAY. Well, we could have some kind of a mechanism. We wouldn't have to specify in the law which ones are friendly and which ones are not. We wouldn't want to offend anybody or make any mistakes.

Attorney General BELL. I don't want to get into an argument with you.

Senator HATHAWAY. If we had some kind of a mechanism where we could agree which ones should be on the list and which ones shouldn't be. I recognize that that could change from day to day, or, maybe hour to hour.

Attorney General BELL. Maybe we could get up a morning list of friendly countries.

Senator HATHAWAY. Well, anyway, it's an area where there is some controversy.

The other area is that although this bill limits itself to wiretapping, it does not apply to hidden cameras or break-ins or anything like that.

Attorney General BELL. Right.

Senator HATHAWAY. Why shouldn't we cover every kind of mechanism that's going to invade the privacy of individuals?

Attorney General BELL. We are preparing legislation on those other areas.

Senator HATHAWAY. Will that be part of this bill, or will it be a supplemental bill?

Attorney General BELL. No, other bills.

Senator HATHAWAY. When will that be ready?

Attorney General BELL. We're working on it now. The next item of priority is electronic surveillance of Americans overseas. We've agreed to do that next. But we're also working right now on the physical searches, too. We plan to cover the whole area.

[Pause.]

But I'm looking at page 7 now where we define electronic surveillance. We've got "electronic, mechanical, or other surveillance device." This would include a camera.

Would it include a camera?

[Consultation with aides.]

It would. These young people with me helped write this bill, and they know more about it than I do. They say that is intended to include a camera.

Senator HATHAWAY. Oh, good.

[Pause.]

Senator HATHAWAY. Or any kind of bug——

Attorney General BELL. But not a search.

Senator HATHAWAY. Not a break-in.

Attorney General BELL. Right.

Senator BAYH. If the Senator would permit me, I was just going to point out that in the bill that we had last year, this language, that we wanted the definition to be broadly inclusive, and I am more comfortable with your second response than I was the first, because it would seem to me that those motion picture camera, still camera, private home, all the kinds of things, we're talking about devices that ought to fit into this definition. We're not talking about the surreptitious entry, this kind of thing.

Attorney General BELL. Yes.

Senator HATHAWAY. I understand now that that is included. Talking about photography——

Attorney General BELL. Television surveillance.

Senator HATHAWAY. Right. Hidden camera, what have you.

And just one last question. I wondered, in the procedure that is established for getting the judge to issue an order—I realize that it's not much different than it is from any other procedure where you get a search warrant—but it seems to me it's extremely important that we protect the rights of people, particularly of our own citizens, from being tapped. I considered last year offering an amendment where we could have someone designated to protect the rights of the individual who is going to be tapped, so it wouldn't be strictly an *ex parte* proceedings, so you would have some adversarial aspect to it——

Attorney General BELL. Yes.

Senator HATHAWAY [continuing]. Like a public defender, only——

Attorney General BELL. I'm not willing to do that.

Senator HATHAWAY [continuing]. Who would be able to appear and be able to contest the allegations made by the Attorney General or his designee.

Was that considered in your draft?

Attorney General BELL. Yes. I've considered it. I'm not willing to do that.

Senator HATHAWAY. Could you tell me why?

Attorney General BELL. Well, as you know, I was a judge myself one time. I passed on some of these matters.

Senator HATHAWAY. I understand.

Attorney General BELL. *Ex parte* always. I looked at the papers. I looked at the Attorney General's certificate, and decided the relevancy. But now we even have more than a judge—and we're going to have a judge under this bill—we've got all these elaborate procedures in the executive department. It's finally up to me as the Attorney General, I pass on it, and some of this information is very sensitive, and as long as we have a safe system, I don't see any need to expand the number of people who are in the information conduit or circle. And I don't see any need for having an adversary proceeding. While somebody is about to get the secrets of the State, we're off having an argument between the public defender and the Justice Department about whether or not we ought to surveil. Some of these things are serious and we just don't have time to have an adversary proceeding. If we're to have to do that, we'd better leave it like it is, and just let the President handle it.

But, as I said earlier, and you may not have been in here at the time, we're willing to give up this power. We want to give it up in the interests of the American people and their rights. But at the same time, though, the President has his constitutional duty, and I just don't see how we can have an adversary proceeding. I just couldn't agree to that.

Senator HATHAWAY. Well, what if it's properly circumscribed so that it's not unduly lengthy?

Attorney General BELL. I've never seen an adversary proceeding that was circumscribed. It's about to break the courts down now.

Senator HATHAWAY. We could draft it that way.

Attorney General BELL. I don't mean to just——

Senator HATHAWAY. No, I understand.

Attorney General BELL [continuing]. Flatly refuse, but that's the way I think now.

Senator HATHAWAY. Thank you. Thank you, very much.

Thank you, Mr. Chairman.

Senator BAYH. Senator Garn.

Senator GARN. Let me go back and make comments on a couple of things that Senator Morgan said.

I think one thing that was left out when he was talking about judge shopping, and I would agree with what you suggested, that it would be a good thing to rotate the judges; I think that would be a good addition to the bill. But we addressed the judge-shopping situation last year in S. 1397 by suggesting that a person could not go from one judge to another if they were turned down. I just wanted to make that point. Senator Morgan has left, but this would further strengthen it. But certainly that was our intent last year. They can go to one judge and that's it.

Attorney General BELL. That's it.

Senator GARN. If they don't like him, they can't say, well, he turned me down, we've got to go to another. That was already in the law.

Attorney General BELL. And it is a real safeguard.

Senator GARN. But I do think it is a good suggestion to go ahead and rotate the judges. We have done that with ourselves. There will be rotation of committee members on the Intelligence Committee, so that we can't stay here for 30 or 40 years even if our constituents decide to keep us in the Senate for that long.

Getting back to all the dialog on the criminal standard on page 4, it seemed to me that when we were writing that last year, that in many cases this almost seems tougher than a probable cause criminal standard. I wonder if you would agree that we can always come up with hypothetical situations—we sat for hours and hours with Attorney General Levi doing the same thing to him that we're doing to you—what about this situation, the case of an airline or whatever, and it seemed to me that all of the hypothetical situations would meet one or two of the tests, but never all. Isn't that the key here, the way it's been defined, that you've got to meet all of the standards. There's one after another, under the direction of a foreign power for example, and there may be some situations, somebody casually going to an embassy that does not meet the standards. I go to an embassy for example and talk to ambassadors. I may be talking to a KGB agent. I don't know. But the point of it is that when you start applying all of those, don't you feel it's rather a strict definition and that it's difficult for an American citizen to meet all of those unless he is deliberately engaged to espionage? Almost be impossible by accident to meet each one of them, wouldn't it?

Attorney General BELL. I think it is an extremely strict standard, and could well be a crime to do those things. If somebody fits all these elements, meets all these various elements, then it seems to me it would be very reasonable for Congress to say that is a crime, and Congress has not gone that far. Nobody is making this a crime.

Senator GARN. Well, of course, I agree with you, but that's the point I wanted to make——

Attorney General BELL. This is a strict standard.

Senator GARN [continuing]. If there was any doubt among the people listening that we have a strict standard in this bill that consists of many different elements, and it would be very difficult for an American citizen to meet accidently all of those tests. In fact, I don't think it would be possible personally to meet all of those tests accidentally. You would have to be deliberately conspiring against the United States to deliver information and all of those things. You just couldn't fit into that category. I suppose all of us at one time or another, particularly those of us in government, might meet one or two of them, accidentally, unknowingly, and we wouldn't want to be surveilled for that. But I just wanted to see if you agreed that it was a very strict definition.

Attorney General BELL. I do agree.

Senator GARN. Getting back to this 1-year category, and I know you recognize what I am going to say, that it's something that we really cannot give sufficient answers here in open session as to why that is needed, but would you agree that it is a very limited area that we carved out, that the vast majority of cases would be involved in the 90-day situation? This is only a very limited area involving extremely sensitive national security situations and to discuss it further would have to be in closed session.

Attorney General BELL. Right, I agree with that. That is my understanding of it, and based on my own experience, I think that's true.

Senator GARN. Indirectly in that 1-year situation, do you feel that the minimization procedures are sufficient to handle that, if indirectly someone else is picked up in that year-long situation?

Attorney General BELL. They already now employ minimization standards in those circumstances. We're very careful to minimize the use of information from any incidental overhear of an American citizen.

Senator GARN. Regarding Senator Hathaway's discussion of an adversary situation, one other point we talked about a great deal last year, there may be one other reason for not having an adversary situation. It may be even more important than the problem of delaying while national secrets were being given away. That is that there would lead to be much less activity or willingness in an adversary position for the Justice Department or law enforcement agencies, to give up information that would prejudice criminal cases. You see, an adversarial relationship may require the disclosure of information which should spoil an investigation and make prosecution impossible.

Attorney General BELL. Yes, that could happen and would happen.

Senator GARN. That's the point I wanted to make, I wanted to see if you agreed that beyond the time delay, that you could prejudice some criminal case prosecutions if you had to go through that procedure.

Attorney General BELL. That's how I happened to hear those in court. They had gotten into the public domain and then the defendant said, well, they prejudiced my case. Listen to my lawyer, listen to me, and then we'd have to have a hearing in camera, no adversary proceeding, to determine relevancy. This is where somebody would be on trial— not as we are discussing here now just to be surveilled, but on trial for their liberty, where they are going to be put in the penitentiary. We didn't have an adversary proceeding. The law doesn't require that.

Senator GARN. Senator Hathaway, if I might just respond to your question of a camera, I think section D is very clear on the camera situation. It says, "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from wire or radio communication." So, it specifically singles itself out from the wiretap, the radio, that kind of thing. It's very clear that "other surveillance device" in that paragraph (D) would have to include cameras. I just wanted to reassure you, if you weren't, that I think that's very, very clear.

I have no other questions at this time, Mr. Chairman.

Senator BAYH. Mr. Attorney General, I don't want to burden you a great deal further here, but I would like to ask you and your staff, if you might, to look at the language in the minimization procedures, where it talks about information relative to a U.S. person being disseminated if it, and the magic words are, "relates to" such subjects as national security or the conduct of foreign affairs.

Now, in order to be able to disseminate that information, the information has to be important or significant. I'm sorry, that's not in the current bill.

We were wondering if we don't need some—I think the word in the present bill is "relevant," and that is such a broad, all encompassing kind of thing, it's almost impossible for me to imagine anything that you pick up that couldn't be construed as relevant, and I wonder if we don't need to give some serious consideration to tying that down to make it "important" or "significant" or something else that's a little bit more than relevant.

You might just look at that and get back to us if you don't have any——

Attorney General BELL. Could we answer that in writing?

Senator BAYH. Yes, that's fine. I mean, I just think that's an area where I think we can tighten up, get away from——

Attorney General BELL. You know, I was just thinking how, if the thing was in my office, how I would know it was important. How would I know that? I would have to get a certificate from the Secretary of State or somebody that knew enough about foreign affairs to know. I could see that it would be relevant, but not assess the importance. We'll answer that.

Senator BAYH. I mean, if it's just relevant, there are all sorts of things where you—you could have a member of this committee talking to an ambassador of a foreign country about something totally unrelated, and this Senator gives his position on that and describes what sort of action he's going to do legislatively which may be contrary to what the administration, whatever that administration might be at the time, would be contrary to the administration's position, so that ambassador then relates that back to the home country and it's picked up and then disseminated because it's relevant because it gives the government more information about what the foreign government has in the way of knowledge about what's going to happen in our Government.

Well, just give that some thought, if you would, please.

Attorney General BELL. We will.

Senator BAYH. I have no further questions at this time. Senator Hathaway, do you have other questions?

Senator HATHAWAY. Just one more.

On page 12, in regards to the application for an order, I understand that if you're asking for a warrant to search somebody's house because there's a certain piece of paper, that you've got to say that you're likely to find it. But there's no assertion in this application of that nature. In other words, what if you tap this person, you're likely to get the information that you say you're seeking, and I wonder why that's omitted? And would you consider putting it in?

Attorney General BELL. We don't want to. We could say that it's likely to produce, you know, we could say that. But I see cases now where nothing is produced, say, in 90 days, and in the next 90 days something is produced, because people may change their habits.

I don't see anything wrong with saying that, because otherwise we wouldn't be doing it if we didn't think it was likely to produce. So we'll work on that with the staff.

Senator HATHAWAY. Good.

Now, there is just one other question that I want to ask you. It relates to what I asked you before about this provision where you can

wiretap in a foreign power for the purpose of "the successful conduct of the foreign affairs of the United States." Now, I suppose you can say, "well, the State Department asked to have that in here," but you are going to have to pass on all of these, and it seems to me that that's an awfully broad category and allows considerable surveillance.

Attorney General BELL. It is——

Senator HATHAWAY. Almost anything can be tied to "the successful conduct of the foreign affairs of the United States."

Attorney General BELL. Well, we'd have to get a certificate from the——

Senator HATHAWAY. What we're really interested in is whether the United States is in jeopardy, whether our national security is at risk.

Attorney General BELL. Well, you know, when you're negotiating a treaty——

Senator HATHAWAY. Although we're interested in it, I don't think we should be conducting wiretaps to get information that would help us "in the successful conduct of the foreign affairs of the United States." It could pertain to just about anything that's going on in that foreign country. I can't think of anything that wouldn't be related in some way to the successful conduct of foreign affairs.

Attorney General BELL. That is broad language. I agree with that. I know that——

Senator HATHAWAY. I realize that State Department witnesses are going to be up and they're going to testify, but I thought I'd ask you, since you're going to have to pass on all these applications——

Attorney General BELL. I believe they can answer it better than I, but I've seen some information that, where you're dealing with one nation which is not friendly with the next nation, and somebody obtains some papers and may give them to the other nation, papers which might cause us great embarrassment and really impede any hope of dealing with the two nations separately. That is the kind of thing that would fit. But this language is broad.

Senator HATHAWAY. Very broad.

Attorney General BELL. Yes. But we would not want to get it to the point where we could not cover the case.

Senator HATHAWAY. I hope that you and your staff will consider some modifications to narrow it down somewhat.

Attorney General BELL. Restrict it.

Senator HATHAWAY. Thank you. Thank you, Mr. Chairman.

Senator BAYH. Senator Garn, do you have anything further?

Senator GARN. No, I have no further questions.

Senator BAYH. Mr. Attorney General, gentlemen, we appreciate your being here and we look forward to working with you until we get this matter in the statute books.

Attorney General BELL. Thank you, very much.

[Whereupon, at 12:04 p.m., the subcommittee was recessed to reconvene at 10 a.m., Thursday, July 21, 1977.]

THURSDAY, JULY 21, 1977

U.S. SENATE,
SUBCOMMITTEE ON INTELLIGENCE
AND THE RIGHTS OF AMERICANS
OF THE SELECT COMMITTEE ON INTELLIGENCE,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:07 a.m., in room 6226, Dirksen Senate Office Building, Senator Birch Bayh (chairman of the subcommittee) presiding.

Present: Senators Bayh (presiding), Stevenson, Hathaway, Morgan, Hart, Moynihan, Garn, and Case.

Also present: William G. Miller, staff director.

Senator BAYH. We will convene our hearings, if you please.

The Rights of Americans Subcommittee of the Senate Intelligence Committee is continuing its hearings this morning on S. 1566, the Foreign Intelligence Surveillance Act. Our witnesses are Admiral Stansfield Turner, the Director of Central Intelligence; Ms. Deanne Siemer, General Counsel of the Department of Defense; Admiral Inman, who is Director of the National Security Agency; Mr. Harold Saunders, Director of the Bureau of Intelligence and Research, State Department; and Mr. Herbert J. Hansell, State Department Legal Adviser. Now, who did I leave out here?

Admiral TURNER. Anthony Lapham, General Counsel of the Central Intelligence Agency, sir.

Senator BAYH. I think that covers everybody. Forgive me for the temporary omission.

We have invited all of you to testify because your agencies have been involved in the development of this legislation, and all of you will have an important role to one extent or another in its successful implementation, I assume, if it is enacted.

However, we also realize that there are aspects of your testimony which touch on classified information. Thus we plan an executive session to handle those matters which you feel we cannot handle comfortably here today.

The State Department has already indicated to us that they would prefer to deal with any questions about the Vienna Convention in executive session. I think this is an approriate request at this time.

The witnesses have been invited to appear as a panel so we can discuss matters relating to several agencies at the same time. We have copies of your prepared statements. You may handle your testimony in any way you see fit, as far as I am concerned.

This of course, is a matter of long term discussion, in which all of you and your predecessors, I assume, have been involved. This committee, Senator Garn and I and others, studied this issue last year.

94-628—78——4

We are starting again. As you know, there is joint jurisdiction between the Judiciary Committee and this committee, and there has been general agreement with the administration on the content of this legislation.

Some of us are still concerned about particular aspects. Some feel we may have gone too far. Some feel we may not have gone far enough in several areas. The best place to start is your reaction to the legislation as it now is, pointing out any concerns you may have, and then hopefully we can address ourselves to some problem areas where we would like perhaps to do a little bit more or perhaps Senator Garn would like for us to do a little less, to see what the impact is going to be.

We want to have, after we are through, legislation that will make it possible for those of you who are charged with the rather burdensome responsibility of conducting the most sophisticated and far-ranging intelligence mechanism in the world to do that in a way that can protect our country, and at the same time do it under guidelines and in a charter and with restrictions that protect the rights of American citizens.

That is not an easy mixture. It is one that tests us, but one I think we must meet and pass. I assume we can.

Admiral Turner, we will let you initiate our dialog here this morning.

TESTIMONY OF ADM. STANSFIELD TURNER, DIRECTOR OF CENTRAL INTELLIGENCE; ACCOMPANIED BY ANTHONY LAPHAM, GENERAL COUNSEL; ADM. DONALD M. SHOWERS, SPECIAL ASSISTANT, INTELLIGENCE COMMUNITY STAFF; AND GEORGE L. CARY, LEGISLATIVE COUNSEL

Admiral TURNER. Thank you, Mr. Chairman, Senators.

I previously indicated my support for this bill in my prepared statement and testimony before the Senate Judiciary Committee in June. I would like to resubmit that statement here, and respond to your request just now, Mr. Chairman, to comment on specific provisions of this bill or items that are not included in this bill.

[The prepared statements of Admiral Turner follow:]

PREPARED STATEMENT OF ADMIRAL STANFIELD TURNER, DIRECTOR OF CENTRAL INTELLIGENCE ON S. 1566

Mr. Chairman and members of this Subcommittee: I welcome this opportunity to testify concerning S. 1566, the Foreign Intelligence Surveillance Act of 1978. I have previously indicated my support for this important legislation in a prepared statement I presented in June to a subcommittee of the Senate Judiciary Committee. At this time I would like to resubmit that statement, with one change noted on page 2, and add a few remarks concerning issues that you identified, Mr. Chairman, in your letter of 1 July inviting me to appear at this hearing, as being of special interest and concern to the Subcommittee. One of those issues has to do with the provisions in the bill covering the certifications that must be made by executive branch officials in support of warrant applications. The other has to do with the appropriateness of amending the bill so as to bring within its coverage electronic surveillance directed at U.S. persons abroad.

First, as to the certification process, I would expect to be among those officials appointed by the President to make the determinations called for by the

bill, regarding the purpose and other aspects of a requested surveillance. Assuming my designation as a certifying authority, I would expect to carry out my responsibilities in much the same way that I do today in the absence of legislation.

As matters now stand, I chair an interagency panel that reviews certain requests to undertake electronic surveillance against foreign intelligence targets. Representatives of the Secretaries of State and Defense serve as the other members of that panel. Surveillance requests are considered at panel meetings attended by the members and other intelligence community officials. In each case the requests are supported by memoranda that justify the operations in terms of standards that closely resemble the targeting standards set forth in S. 1566. In no case is any request approved except after consideration at a meeting of the panel and except after review of the justification memorandum. During my term of office there has been no occasion in which approval was given to all requests considered at any one time, a point I make to indicate that the process is careful and selective. Approved requests are forwarded to the National Security Adviser to the President, and those that receive his endorsement are in turn forwarded by him to the Attorney General for review and final approval. Each final approval is valid for only 90 days, and consequently the entire review process is repeated at 90-day intervals with respect to each surveillance activity requested for renewal.

Should S. 1566 become law I can assure the Committee that I woul continue to devote my personal attention to matters within my authority as a certifying official, and I envision that I would base my certifications on review and approval procedures akin to those that are already in use.

Second, as to the idea of broadening the provisions of the bill so as to make them applicable to electronic surveillance activities conducted abroad, I believe that such a step would be inappropriate and unwise. In my view the circumstances that are relevant to the gathering of foreign intelligence and counterintelligence information abroad, including the acquisition of such information by means of electronic surveillance, are materially different from the circumstances surrounding such activities when conducted in the United States. A critical difference is that activities conducted abroad are heavily dependent on the cooperation of foreign governments and foreign intelligence services, and any enlargement of the scope of the bill to cover such activities could have far-reaching consequences in our relationships with those foreign governments and intelligence services.

In its present form the bill deals comprehensively with a large and complex subject, namely all types of electronic surveillance carried on in the United States that are not already regulated by other legislation. Electronic surveillance abroad is another large and complex subject in itself, and I believe it should be left to separate legislation, which as you know this Administration is now engaged in drafting.

STATEMENT OF ADMIRAL STANFIELD TURNER, DIRECTOR OF CENTRAL INTELLIGENCE, AT HEARINGS BEFORE THE SUBCOMMITTEE ON CRIMINAL LAWS AND PROCEDURES OF THE JUDICIARY COMMITTEE OF THE SENATE ON THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1977

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 be 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 overreaching 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 one of policy.

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 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 issurance 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, as 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 proposed legislation as desirable and urge its early consideration and adoption.

In your letter to me of the 1st of July, asking for an appearance here, you mentioned two points that I think merit a small comment before we proceed. The first is the question of the certification process which is prescribed in the bill, and the second is the question of whether the bill should be extended to cover electronic surveillance against Americans abroad.

On the first part, the certification procedures, I would expect to be one of the officials designated under the provisions of the bill to make determinations regarding the purpose of the requested surveillance. Assuming that I am so designated, I will expect to carry out my responsibilities in the future in a manner very similar to that which is performed today.

Today I chair an interagency panel on which both the State Department, the Defense Department, and other appropriate agencies as necessary are represented. That panel reviews all surveillance requests at panel meetings. Those requests must be supported by memorandum that justify the operations in terms of standards that closely resemble the targeting standards which are set forth in the bill before us today.

In no case is any request approved except after an actual meeting of the panel and after a review of these memorandum of justification. During the relatively short time I have been here, I would point out there has been no meeting of the panel at which all of the requests before it were approved. I mention that only to say that this is not a rubber stamp process. Once approved, these requests are sent to the National Security Adviser to the President. If he further approves them, they are forwarded to the Attorney General for final approval. Each approval lasts for 90 days, and thus we must renew these and go through this procedure again every 90 days.

Should this bill become law, Mr. Chairman, I would anticipate devoting my personal attention to these matters in much the same way as I do now, and I believe these procedures are very solid.

On the second subject of extending this bill to cover Americans abroad, I believe that would not be appropriate at this time. The circumstances that are relevant to the gathering of foreign intelligence and counterintelligence information abroad, including the acquisition of such information by means of electronic surveillance, are materially different from the circumstances surrounding such activities when conducted in the United States. A critical difference is that the activities conducted abroad are heavily dependent upon the cooperation of foreign governments and foreign intelligence services.

Any enlargement in the scope of this bill to cover such activities could have adverse consequences in our relationships with these governments and intelligence services. In its present form, this bill deals comprehensively with a very large and complex subject, namely, all types of electronic surveillance carried out in the United States not already regulated by other legislation.

Electronic surveillance abroad is another large and complex subject in itself, and I believe that it would be better to handle this in

separate legislation. I believe the Attorney General has mentioned to you that the administration is pledged to prepare this legislation in an appropriate time frame.

Thank you, Mr. Chairman.

Senator BAYH. Do the other members of the panel mind if we address ourselves to the Admiral here right now? He has another legislative responsibility shortly, as indeed does the Chairman of this subcommittee. I am hopeful my colleague, Senator Garn can help keep a hand in the dike here. Do you mind, gentlemen and Ms. Siemer, if we address a couple of questions to the Admiral here first?

Have you been consulted or is your staff now preparing to make a contribution to this legislation that the Attorney General referred to?

Admiral TURNER. Yes, sir, we are actively participating in that decision process.

Senator BAYH. What concerns me is, I am convinced you are sincere, and the Attorney General and the President are sincere that we will have other legislation to deal with this, but frankly, I don't know how much gas we have in our gas tank as far as legislative resolve to deal with this problem. It is a very difficult one across the board, and I think there are abuses that could exist, and as my distinguished colleague, Senator Garn, has mentioned, there is no law now covering it.

Once we have legislation covering the bulk of the problem, then I wonder how much effort we are going to have, how much support we will have for additional legislation to cover what is a relatively small part of the problem. How far along are you in your deliberations on this?

Admiral TURNER. It is very difficult in any bureaucratic process to predict how close you are to the finish, because you can have almost all the work done and the last 10 percent may take 50 percent of the time. I think we are quite well along, but there could be some critical decisions ahead that will be difficult to iron out between the various interests involved. I assure you that there is no dilatoriness involved. We are proceeding as rapidly as we possibly can with due account for the various interests concerned.

Senator BAYH. I certainly don't mean to imply any dilatory tactics. This is a difficult problem, and it affects the ability of you and your people to do your business. What I would think might be helpful, and I am sure part of it is not at all appropriate here, but I would like for us to be more definitive than the response you have given. I would like to know specific case histories. You can strike the name and serial number out of them, but I would like to know just why it is not possible for us to be able to at least move forward in a couple of areas that I will address myself to. Could you give some specific examples that show that applying the same kind of protection to American citizens abroad would be too onerous?

We do not leave our citizenship at the coastline. I am sure you realize that. When you talk about the panel, Admiral, would you rather do this in executive session, or can you tell us, when you say not all of the requests granted—or all requested have been granted, how many are we talking about? I would like to know, targeting Americans when they are abroad, what are we talking about, or can we talk about that?

Ms. Siemer, are you shaking your head, don't answer, or none?

Admiral TURNER. At the present time the panel does not concern itself with surveillance of Americans abroad. That is a different procedure. We are talking about electronic surveillance in the United States as covered by this bill, as covered in the analogy I drew in my opening comments with this panel, sir.

Might I add one point? I am, of course, not in a position to judge how much the legislative traffic will bear here as to whether there will be adequate interest if the bill comes up separately, but my particular interest from an intelligence point of view with overseas surveillance is protecting our relationship with these foreign agencies, because it is almost out of the question to perform this kind of activity without their cooperation.

In my view, separating the bills will help us, because any bill we pass regarding foreign surveillance of Americans aboard will to some degree inhibit these relationships. These agencies, particularly after all the disclosures we have had in public in this country in recent years regarding our intelligence activities, will be wary of continuing a relationship with us, but it would be an easier explanation for us if there was a discrete bill that handled just the foreign aspects of things, so there was no confusion with the procedures in the United States.

Senator BAYH. I would think, Admiral, insofar as the discreteness and the separate nature, I think we could make it very clear as a part of this package that we are talking about a different problem, really a different mission. I guess we are going to have to resolve in our own minds how much traffic the legislative mule will bear. Maybe that question about the size of the burden had best be left to executive session, where we are going to meet next week——

Admiral TURNER. All right, sir.

Senator BAYH [continuing]. And if we can, have a discussion of some of the specifics so we will know just exactly in more detail what we are talking about here. Let me deal with two types of areas that I addressed to the Attorney General. What about minimization? Would it not be possible by requiring appropriate minimization to alleviate or greatly lessen the danger of this information being abused as it is collected? In other words, if we are talking about an American citizen that is targeted or picked up even coincidentally by a foreign agency, there is not much we can do about that, particularly unless we initiate it or are advised about it in advance. The concern we have is, what happens to that information, or what is likely to happen if it is stored improperly in one of these big computer systems?

Now, if we could say that we would use the same standard of minimization, if it involved an American citizen, if that information is picked up abroad, it seems to me we would have gone a long way to eliminating or alleviating possible abuse.

Admiral TURNER. We are in agreement with you, Senator, on the desirability of minimization procedures, and minimization procedures are in effect today under the direction of the Attorney General of the United States with regard to all Central Intelligence Agency electronic surveillance abroad. So, as to your suggestion that we might put it into this legislation, I would not have a fundamental objection. I would say I do not think it is an urgent issue, since we are following

minimization procedures already, and that it would be better to incorporate it in the bill that contains all other matters regarding electronic surveillance abroad, rather than to mix apples and oranges.

Senator BAYH. I hope you will excuse me. I have an Appropriations Committee meeting.

Admiral TURNER. Thank you, sir.

Senator GARN [presiding]. Admiral Turner, I wonder if I might ask about this discussion which we might pursue further in executive session about the legislative load. We are really dealing with two questions here: On the one hand, what interest will there be in a spearate bill if we do not address the foreign aspects at this time; but the other question is really, if you load it up, do you get any bill at all? Now, I fall on that side of it, strictly from a political standpoint, which we can't ask you to judge. That is in our realm. I think we are in such a critical balance on this bill and votes on the floor, at least it is my opinion, purely from a political standpoint, forgetting the merits, which we will talk more about, that we load it up too much and it may be the straw that keeps the bill from passing on the Senate floor.

That brings me to another point about the balance of this whole bill. Senator Bayh and I have been involved in it for over a year now, and getting to that balance of where you adequately protect the rights of American citizens but still not inhibit too much the legitimate intelligence-gathering activities that are necessary for national security, so we are on a very teeter-tottery situation there as far as votes, too.

In this committee, the division is very close, Senator Bayh and I are both cosponsors of this bill. He would like to tip it a little more towards more protection of the individual, and I would like to tip it a little more back the other way for legitimate intelligence-gathering activity. So what we are really dealing with for all of you as we look at this is, right now, I think it is about where it needs to be, and if we tip it one way or another, you start losing votes on the liberal or so-called conservative side so you don't get any bill at all. That is after months of discussion last year. I think we have reached sort of a compromise or a balanced position some place in the middle, that if we tinker with it too much one way or another we are just not going to have any.

I do think we need something. I think, as I said yesterday that we have no law at all controlling these activities. That is why I puzzle a little bit with some of the groups who want tough criminal standards for using this, because apparently they would rather have the present situation than no bill at all, which I don't understand, where we have almost no protection for the individual American citizen at this time.

Let me ask you a couple of questions. In your statement before the Judiciary Committee, on page 4, you stated that it is possible, for example, that the bill's definition of foreign intelligence information will prove too narrow or will be too narrowly construed to permit the acquisition of genuinely significant communications. Can you tell me what part of the definition you are referring to, and does the definition require that certain information be essential to national security or the conduct of foreign policy? I share your concern.

Admiral TURNER. Well, it is the word "essential" on page 5, paragraph 5–B, and how that is construed, Senator, that is going to be a critical point when this bill is interpreted.

Senator GARN. Well, your fear is that it could be too narrow and restrict you too much?

Admiral TURNER. That is a possibility. I think a lot depends on the legislative history and how that is written regarding what the committee really interprets as the meaning of "essential," because you can stretch "essential" to be very, very narrow.

Senator GARN. Do you have any specific suggestions then how we could clarify the legislative intent so that we make certain that that particular word or foreign intelligence information is not interpreted too narrowly?

Admiral TURNER. It is my understanding that there has been a general agreement on the wording of the report on this point. That will help a good deal.

Senator GARN. Well, if you do not have specific answers now, certainly in writing. It is an area that I agree with you could be too narrowly interpreted or too broadly, and if you can help us in being specific here, so that again we reach that proper balance, we would be grateful for that.

Admiral TURNER. All right.

Senator GARN. You have already described your current situation on Executive branch review procedures providing for review by this interagency panel, including you, the Secretaries of State and Defense, every 90 days. Would you expect that this procedure for 90-day review will be changed if the bill is enacted to provide court orders lasting for as long as a year? Now, we did do the dual situation with 90 days, and also the year in specific situations.

Admiral TURNER. My personal inclination, and this is not entirely under my authority, so I cannot promise or guarantee this, would be that we would continue with the same procedures we have now, reviewing at 90-day intervals, even though we would only be required to go back to the courts on a yearly interval for the one type of surveillance.

Senator GARN. Do you find in this interagency group the 90-day periods would be burdensome to you?

Admiral TURNER. Not unduly. It is obviously a burden, but the load is not that heavy. When I say that, I want to say with great sincerity that it has got to be a burden, because you have got to take it seriously. If it becomes too little a burden, that means you are passing over things lightly, and we cannot afford to do that, but I think we are willing to accept that degree of burden, sir.

Senator GARN. Not nearly the burden that we apply on the executive branch of Government to constantly appear before congressional committees, I suppose.

Admiral TURNER. I will take the Fifth Amendment on that, sir.

Senator GARN. We give you little time to work.

I have no further questions at this time, Senator Morgan?

Senator MORGAN. Admiral, we will try again. As I understand your statement, you say that surveillance of foreign intelligence is now being carried out by your agency without a judicial warrant in the United States.

Admiral TURNER. In the United States, yes, sir. If you say my agency, it is not done by the Central Intelligence Agency. In my hat as the Director of Central Intelligence, yes, it is being done.

Senator MORGAN. And you say this is done under a written delegation of authority from the President, which I assume that you feel he has the inherent right to do.

Admiral TURNER. Yes, sir.

Senator MORGAN. How far does the inherent right of the President to direct electronic surveillance of American citizens go in the interest of national security?

Admiral TURNER. In my view he has the right to conduct such surveillance as he believes is necessary, but what we are all doing here, and the President supports this general measure, is to lay down the guidelines, the rules under which he will operate in the future.

Senator MORGAN. I think we all agree that this President is trying to do what is within reason, but I think we are trying to write a law that will last for years to come, which might encompass and would encompass the terms of office of other Presidents.

Admiral TURNER. Yes, sir.

Senator MORGAN. But it is your feeling, then, that the President has an inherent right to do whatever he in his judgment thinks is necessary in the area of electronic surveillance, as long as it is done in the interest of national security?

Admiral TURNER. My answer to that is generally yes, but I would like legal advice to make sure I haven't left out a nuance here.

Senator MORGAN. I say to you, Admiral, in my own mind I have a great deal of reservations about that, and I asked the Attorney General yesterday if he had a brief stating his position, and that is why I am pursuing it today, and then I was going to ask if you had any briefs prepared on this.

Admiral TURNER. We don't have a brief of our own, and if I were asked to produce one, I would almost have to go to the Attorney General to get the authoritative one.

Senator MORGAN. Does counsel have an opinion as to how far or whether or not there are any limitations on the President's inherent right to engage in electronic surveillance so long as he is doing it in the interest of what he believes to be national security?

Admiral TURNER. I am certain, Senator, that there are limits on any inherent power that may exist, but under the delegation that you have referenced, the sorts of electronic surveillances that are carried out are already limited in much the same way as they would be limited by the terms of this legislation.

Senator MORGAN. I understand that, but I am looking down the road. In the electronic surveillance that you are now carrying out, would the need for that surveillance or the reason for it meet the criminal law standards or standards of probable cause?

Admiral TURNER. I believe it would meet the standards of probable cause, Senator. In many instances it would not meet a criminal standard, and indeed in many of the instances in which the surveillance would be conducted pursuant to the legislation there would be no requirement that a criminal standard be met. I am talking now principally about surveillances conducted against those organizations or entities defined as foreign powers under the bill.

Senator MORGAN. Well, I understand that, and that is one of my concerns about this legislation, whether or not we should require it.

Can you give me an example in open session—if you cannot, we will wait until later—of a type of surveillance that you are now carrying out against American citizens in this country which would not meet the criminal law standards, and then a type in which you could meet them?

Mr. LAPHAM. Senator, I think that question would be better put to the FBI. The Director is not involved in the approval of any surveillance directed against a United States person in the United States.

Senator MORGAN. Did I not understand you, Admiral, to say that you did sit on the board or would sit on the board of certification with regard to the need for electronic surveillance?

Admiral TURNER. On foreign intelligence, Senator, not on domestic intercept of United States citizens.

Senator MORGAN. Now, when you say foreign intelligence, are you talking about surveillance conducted in foreign countries?

Admiral TURNER. No, sir, surveillance conducted against foreign entities in the United States.

Senator MORGAN. Well, that is what I am asking you for. Well, that would necessarily or could involve American citizens, could it not?

Admiral TURNER. If it does, we come under the minimization procedures here. We do not target American citizens for this purpose.

Senator MORGAN. How about an employee of a foreign entity, such as Air France, one that is frequently referred to, an American employee of Air France?

Admiral TURNER. That we have to leave to the FBI to handle.

Senator MORGAN. Even though you are seeking it for foreign intelligence?

Admiral TURNER. Yes, sir.

Senator MORGAN. Now, you said not all requests that have been made have been approved. Can you give me any idea of the frequency of the requests that are made? How much electronic surveillance do we do in this country for foreign intelligence purposes?

Admiral TURNER. I prefer to talk about the quantities in executive session, sir. I would only say that when we review these every 90 days, there is always one or more that we have some question about, and do not approve. That is what I was trying to get at.

Senator MORGAN. Admiral, I know you are in a hurry, and we will pursue this later, but let me just give you my thoughts. The more I study the bill and the more I study and recall the testimony during the 18 months of the Church Committee, the more I am inclined to believe that in the Harlan Stone line, that there ought to be a criminal standard, either reasonably, either the person is committing a crime or is about to commit a crime, and I am not so sure that almost every purpose that you surveil for would not meet those standards.

I know there is some question as to how you interpret national defense, as narrow as it was interpreted in 1941, or whether you would interpret it in light of more recent court decisions, but when we come back in executive session, those are some of the questions I would like to pursue with counsel and with you.

Admiral TURNER. Thank you, sir.

Senator MORGAN. I have no further questions.

Senator GARN. Senator Case, do you have any questions?

Senator CASE. No questions, Mr. Chairman.

Senator GARN. Senator Hart?

Senator HART. Only a couple of questions, Admiral, regarding congressional oversight, which we got into a little bit yesterday with the Attorney General. Of the varying proposals concerning last year's bill and this year's, and so forth, concerning reporting requirements to appropriate committees of Congress, including this one, most have contained provisions having to do with reporting that is limited to the number of applications for orders and the number of orders granted. Do you believe that is adequate for this committee's purposes, or do you believe this committee should have the authority to get more specific information about the nature of the orders applied for and granted, the details of the case, in other words?

Admiral TURNER. I certainly think the committee has the authority and can obtain as much detail as necessary. I have some reluctance, Senator, to see us engrave into legislation the specific types of information that will be provided Congress. In particular I have felt that the exchange of information and the overall relationship between the Senate Select Committee and the intelligence community has been developing so well, and we have been working out reporting procedures, that it seems to me it is better to keep it on that basis rather than get something in legislation here that would be more difficult to change if we did mutually want to change it in the future.

Senator HART. Therefore, it is your understanding that there presently exists under Senate Resolution 400 or other authority, authority for this committee to request from you and other elements of the Intelligence Community information regarding electronic surveillance, and that authorization in legislation of this sort would be more by way of limitation than anything else.

Admiral TURNER. Yes, sir, and my understanding is that the detailed reporting procedures that we are talking about are under negotiation now between the Justice Department and the staff of your committee. While these would not go into the legislation, they will be very specific so that there is no ambiguity when this bill is enacted.

Senator HART. We constantly have to make, and I think Senator Morgan appropriately made the point about the differences between and among personalities and Administrations and Congresses, and that the intent of one Administration may be benign and the next not so benign, and I think the problem here is how to construct a rule of law and a set of procedures which will govern those who may not have the same intent and the same understanding of the present law that you and this present Administration have, and that is a matter, I think, of concern, that even though all of us seem to be working all together now, no one here today is going to be here forever, and we have to guarantee somehow that future committees, future members of this committee, future Directors of the Central Intelligence Agency, and future Presidents have the same relationship, and this committee has the same access to that kind of information. I think that is the problem.

Let me just ask one correlated question, and that is whether you have a system for evaluating the returns on electronic surveillance of foreign sources at the present time, of going back and determining whether in retrospect that surveillance was worthwhile and the information gathered was beneficial compared to the risk taken.

Admiral TURNER. Yes, sir, we do that every 90 days, specific for each target.

Senator HART. And has that resulted in any case in your judgment that for one reason or another the risk taken or the—well, any legal questions that may have arisen outweighed the results that you obtained?

Admiral TURNER. Yes, it has.

Senator HART. And that in turn is factored into future decisions?

Admiral TURNER. Yes, sir, that has led to cessation of authorization.

Senator HART. And a decision, in fact, not to even seek authorization in some cases?

Admiral TURNER. When we do that evaluation, Senator, it is because it is an ongoing activity, and then if the evaluation says the risk is too high, we cancel it. We also make a risk evaluation of a proposed surveillance. We cannot evaluate what we collected, but we can evaluate what we might collect against what the risk would be, and in both instances I don't think I have been to a meeting in either one of those in which something hasn't been turned down. Is that your recollection, Hal?

Mr. SAUNDERS. That is certainly true.

Admiral TURNER. Yes.

Senator HART. Thank you very much.

Admiral TURNER. In short, if we have enough meetings there will be nothing left.

Senator HART. That might be good.

Senator GARN. Admiral, may I ask you, in light of several questions from different Senators, and we need to handle it in executive session, but it might be well if you could when you come back for that session provide us maybe with some written examples or synopses of your committee meetings, of what you have approved and have not for the executive session, so they could have their questions more specifically answered, if that would be possible.

Admiral TURNER. Yes, sir.

Senator GARN. Senator Case?

Senator CASE. Thank you, Mr. Chairman.

Admiral, I do not want to repeat anything that has been done before, before I got here, but I was interested in that question of whether in regard to foreign surveillance and also information picked up accidentally, whether the minimization provisions of the present bill might not apply to them before a complete statutory framework is set up as you propose under new legislation.

Admiral TURNER. Yes, sir, we believe minimization procedures should be included in the regulation of foreign electronic surveillance. We do follow such procedures today with respect to CIA intercepts overseas, and my only hesitation is regarding whether minimization procedures for foreign electronic surveillance should be incorporated in this bill, which is basically domestic. When we come to a bill for the foreign intercepts, we would favor a minimization procedure.

Senator CASE. But is there any reason why the minimization procedures should not be made applicable in this bill to those categories without waiting for a whole new legislation governing generally the question of surveillance abroad?

Admiral TURNER. No strong objection to it. I think it is mixing apples and oranges; I would prefer to treat the issues regarding electronic surveillance abroad in one bill. It is a matter of tidiness.

Senator CASE. What about minimization procedures being made applicable to information accidentally acquired in the course of other wiretapping here in this country? Is there any reason why that should not be made applicable?

Admiral TURNER. No, sir, not in my opinion. I think it is already.

Senator CASE. Thank you. I do have a few more questions, but I want to read the record before I ask them, so if I could I would like to have them submitted for the record.

Senator GARN. At this point, Admiral, what I would like to do is go on with the prepared statements of some of the other witnesses, recognizing that you have another legislative commitment. If you would stay with us in case there are other questions as long as you can, and without further questioning or statements, when you feel you have to leave, feel free to just get up and depart, and we will understand why you are going.

Admiral TURNER. Thank you, sir.

Senator GARN. At this time, we would like to ask Ms. Siemer if she would present her statement.

TESTIMONY OF MS. DEANNE C. SIEMER, GENERAL COUNSEL, DEPARTMENT OF DEFENSE; ACCOMPANIED BY ADM. BOB INMAN, DIRECTOR, NATIONAL SECURITY AGENCY; AND ROWLAND MORROW, DIRECTOR, COUNTER-INTELLIGENCE, DEPARTMENT OF DEFENSE

Ms. SIEMER. Thank you, Senator.

I appreciate the opportunity to appear before you today as the representative of the Secretary of Defense to testify with respect to S. 1566, the proposed Foreign Intelligence Surveillance Act. With me is Admiral Bob Inman, the Director of the National Security Agency, and Rowland Morrow, who is head of DOD Counterintelligence is also with us, if there are detailed questions on that subject.

When Secretary Brown testified before the Judiciary Committee, he described in detail the procedures that the Department will use if S. 1566 is enacted. He also emphasized the importance to the Department of Defense of the provisions of the bill that protect the security of intelligence information once it enters the judicial system. If it is acceptable to the committee, the Department would like to submit the Secretary's prepared statement as part of our statement before this Committee.

Senator GARN. Without objection, we will be happy to include that in the record.

[The prepared statement of Harold Brown follows:]

PREPARED 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 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 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 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 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 would 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 needed 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 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:

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.

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.

Ms. SIEMER. If it is acceptable to the Committee, the Department would also submit the rest of our prepared statement for the record, and we will move on to answer questions.

Senator GARN. It is so ordered.

[The prepared statement of Ms. Siemer follows:]

PREPARED STATEMENT OF HON. DEANNE C. SIEMER, GENERAL COUNSEL, DEPARTMENT OF DEFENSE

Mr. Chairman, I appreciate the opportunity to appear before you today as the representative of the Secretary of Defense to testify with respect to S. 1566, the proposed Foreign Intelligence Surveillance Act. With me is Admiral Bob Inman, the Director of the National Security Agency.

When Secretary Brown testified before the Judiciary Committee, he described in detail the procedures that the Department will use if S. 1566 is enacted. He also emphasized the importance to the Department of Defense of the provisions of the bill that protect the security of intelligence information once it enters the judicial system. If it is acceptable to the committee, the Department would like to submit the Secretary's prepared statement as part of our statement before this committee.

Most of the complexities of the bill arise out of provisions that are intended to govern the counterintelligence activities of the FBI because these activities are more likely to involve surveillance of Americans. While the Defense Department conducts military counterintelligence activities within the United States, the only non-consensual electronic surveillance conducted in connection with these activities in the United States is done by the FBI.

The Department of Defense also has substantial functions in collecting positive intelligence as distinct from counterintelligence. The Secretary of Defense is the executive agent for signals intelligence activities on behalf of the Executive Branch. These activities are carried out by the National Security Agency, some within the United States. The military departments do not conduct electronic surveillance for positive intelligence purposes within the United States.

Signals intelligence operations covered by this bill are directed against the types of foreign powers defined by subparagraphs A, B and C of Section 2521 (b)(1)—that is foreign governments, factions of foreign nations, and entities that are openly acknowledged by foreign governments to be directed and controlled by them. These operations do not involve the targeting of individuals and are not directed against the communications of Americans.

The intelligence gained from these activities is of critical importance to the Department of Defense and other users of intelligence. The protections of this bill that are designed for Americans and resident aliens will not impair these operations against foreign powers if they are not extended to situations where there are only remote possibilities that communications by Americans will be acquired. The bill contains a careful dichotomy which provides more stringent requirements for targeting the types of foreign groups in which Americans might be involved, and less stringent requirements for targeting foreign governments and their entities where, on the basis of past experience, Americans are never the communicating parties. Different standards are applied to the information required to be set out in the application, the extent of the certification, the substance of the review by the court, the duration of the order, and the information to be produced in support of extensions of orders. It is important to the capability of the Department of Defense to provide effective foreign intelligence that this dichotomy be maintained.

The positive intelligence information sought through signals intelligence operations is almost entirely that described by subparagraphs A and B of Section 2521(b)(5)—information relating to the ability of the United States to protect itself against hostile acts, to the maintenance of national defense or security, or to the successful conduct of foreign affairs.

The bill contains a difficult differentiation in this regard. The definition of "foreign intelligence information" includes information that is necessary to protection against a hostile attack and information that is essential to the national defense or the conduct of foreign affairs. It is of great importance to the signals intelligence effort that the Committee make clear that information can be necessary or essential in the context of the national defense because of its relationship to other information—either in determining the value of other information or completing a data series necessary to an assessment. In dealing with signals intelligence from foreign government sources, it seldom occurs that any one message or any one source can, standing alone, meet either the "necessary" or "essential" test. But put together, a number of messages or information from a number of sources can provide extremely valuable intelligence that plainly meets either test. A fair and clear explanation by the Committee of the "necessary" and "essential" requirements will set the standards high enough so that not every bit of information about any foreign government would qualify as foreign intelligence information—but not so high as to cripple the signals intelligence effort, which by its very nature requires fitting together pieces of information to discover the shape of the whole.

The Defense Department conducts electronic surveillance against foreign powers both in the United States and overseas. The geographic distinctions now included in the bill are important to the Department. This bill was designed to

deal with the problems of electronic surveillance of Americans within the United States. An amendment to graft onto S. 1566 provisions dealing with electronic surveillance overseas would be opposed by the Department of Defense for the following reasons:

First.—Trying to accommodate all of the differences between foreign and domestic electronic surveillance in one bill would make the law very complex. 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.

Second.—Cooperative foreign intelligence arrangements with allies are important to the intelligence effort. Controls on electronic surveillance overseas must be drafted carefully so as to take into account circumstances created by these agreements and to avoid, where possible, adverse effects on these intelligence sources.

Third.—The laws of foreign jurisdictions create special problems. In some countries the legal requirements and procedures involved are substantially different than United States law with respect to electronic surveillance, and the expectation of privacy is often also substantially different.

Fourth.—Many Americans overseas are military personnel, and electronic surveillance, both on-base and off-base, of military personnel presents special problems in both law enforcement and intelligence contexts.

Fifth.—The problems of identifying U.S. citizens and resident aliens, as such, when they are abroad is very difficult, particularly in signals intelligence work.

Sixth.—The very restrictive definition of "agent of a foreign power" appropriate to limit surveillance in the United States should be expanded to cover other U.S. persons whose overseas activities may be of legitimate foreign intelligence interest, such as defectors to Soviet bloc nations and officials of foreign governments who also hold U.S. citizenship.

The Department of Defense believes that a workable bill to govern electronic surveillance of Americans abroad can be drafted, and my office is now working with the Department of Justice on such a bill.

The Department of Defense believes that S. 1566, in its present form, would successfully create a workable, effective system for protecting the rights of Americans and, at the same time, preserve the effectiveness of the very valuable foreign intelligence and counterintelligence capabilities of the Department of Defense.

Thank you.

Senator GARN. Senator Morgan?

Senator MORGAN. I have no questions.

Senator GARN. Senator Hart?

Senator HART. No questions.

Senator GARN. Senator Case?

Senator CASE. You rendered me almost speechless as you are by your brevity. I commend you for it. I want to read this, and then I would ask any questions I might have.

Ms. SIEMER. Senator Case, I might be able to help with one of the questions.

Senator CASE. If there is anything you want to emphasize, go ahead and do it.

Ms. SIEMER. One of the questions you asked was why we simply shouldn't engraft on this bill minimization procedures with respect to international communications that are not covered by this bill. One of the problems, as Admiral Turner has emphasized, is, that it brings into this bill all the complicated definitions that will be needed in the foreign bill, and there is one good example of that, that I could point out here. If you look at page 28, under section 4(f), it applies to acquisition by the U.S. Government of these kinds of communications.

Now, the problem we would have if we engrafted minimization procedures formally in this bill, as Admiral Turner has told you, is

that we already apply minimization procedures to these through the Attorney General's requirements.

If we do it formally with respect to this bill, we will be required to define the term, "by the United States Government." Does it involve only situations when the United States acts alone, or when it acts in concert with other governments, or when there is some cooperation but not in concert? There are a great number of shades of difference there of those kinds of operations which are difficult for us to define. We think you have sufficient protection in the Attorney General's current procedures, and that those definitions will be made applicable in a bill that deals only with foreign communication or international communications interception abroad. That will provide the kind of clarity and guidance that our intelligence agencies need to be able to know precisely what the requirements are.

Senator CASE. Would your concern apply also to the application of minimization procedures to information accidentally or collaterally obtained, not in connection with people examined abroad?

Ms. SIEMER. No; it does not.

Senator CASE. I think that is all. Thank you.

Senator GARN. With the approval of the Committee, I think we might expedite by asking Mr. Saunders and Mr. Hansell to proceed with their statements, and then we will be able to ask questions of any of the witnesses. Mr. Saunders, if you will go ahead with your statement, and handle it in any way you would like.

TESTIMONY OF HAROLD SAUNDERS, DIRECTOR OF INTELLIGENCE AND RESEARCH, DEPARTMENT OF STATE

Mr. SAUNDERS. Yes; with your permission we would like to present a joint statement with me concentrating on the intelligence aspect of the legislation, and with Mr. Hansell the Department's legal adviser, talking about the legal aspects of the bill.

We welcome the opportunity here to put formally on the record the State Department's support for this legislation, the Foreign Intelligence Surveillance Act of 1978. We support this bill for two broad reasons. First of all, we support it because we believe it will create a clear statutory basis for the conduct of electronic surveillance for foreign intelligence purposes. As such, we believe the enactment of this bill can do much to restore the faith of the American public in the Intelligence Community and in our government as a whole, including the ability of the Congress and the Executive branches to work together to protect liberty and security.

Our second reason is that, having the need to form a statutory basis for this kind of activity, we believe that in this bill there is a correct balance between the needs of a free society to maintain a strong foreign intelligence service and capability and the rights of citizens and inhabitants in a free society.

We see some risks in the bill, the risks that it might be interpreted in the courts in such a way as to render us unable to obtain the intelligence information we think necessary, but we feel that those risks are manageable and that the risks are worth taking in the light of the objectives which we have in proposing the enactment of this bill.

The bill also, we believe, has the additional advantage of eliminating the risk that the authority to conduct electronic surveillance without a warrant would be abused. We note and support the fact that the bill requires the Executive branch to meet very high standards in the certification and application for a warrant. These are procedures which, as Admiral Turner has indicated, we are following now. The procedures in the bill are nearly identical to those standards which are being followed now, and our feeling is that one of the strong points in the bill is that it codifies these stringent requirements into law, and we welcome that.

Finally, the committee, I am sure, appreciates the importance of foreign intelligence activities that will be conducted under the criteria and procedures of this legislation. These activities form an integral part of our total foreign intelligence effort, and they contribute information required to [the] support [of] the process of formulating and carrying out the foreign policy of the United States which is the responsibility of the State Department.

I am confident that the information needed for this purpose can be acquired within the terms of this bill without violating the rights of United States persons. I am also confident that the committee appreciates the sensitivity of going into an evaluation of the product of this activity in open session, but we will be prepared in executive session, to the extent the committee wishes, to share with Admiral Turner in answering the questions that have already been posed, namely, what is the evaluative process, how does this kind of material contribute to the conduct of foreign relations, and I think we can examine that just as fully as you wish next week, and we will be prepared to be quite concrete in any ways that you wish.

That is the extent of my comment. I would be prepared to answer questions. Mr. Hansell has a few comments about the legal side of the bill, if he may proceed.

TESTIMONY OF HERBERT J. HANSELL, LEGAL ADVISER, DEPARTMENT OF STATE

Mr. HANSELL. Mr. Chairman, Senators, you have copies of my prepared statement, and since it deals mainly with issues that you have already addressed either this morning or in the session with the Attorney General, I am inclined to think we would advance the objective if I simply submit that statement for the record, and go forward with your questions, which I am certainly happy to do.

Senator GARN. We will make certain that all of your prepared statements are printed in full in the record.

[The prepared statements of Harold Saunders and Herbert J. Hansell follows:]

PREPARED STATEMENT OF HAROLD SAUNDERS, DIRECTOR OF INTELLIGENCE AND RESEARCH, DEPARTMENT OF STATE

Mr. Chairman, I welcome the opportunity to appear before this Committee and testify on behalf of the State Department in favor of S. 1566, the Foreign Intelligence Surveillance Act of 1978. The Department fully supports the enactment of this important legislation.

I would like to propose a joint presentation today with Mr. Herbert J. Hansell, the Department's Legal Adviser, sharing the witness chair. I will address my remarks to the impact of this legislation on intelligence matters and Mr. Hansell, will address the legal aspects. Both of us propose to make very short statements and then will be happy to answer any questions the Committee might have.

We note, Mr. Chairman, that you have scheduled executive session hearings for next week and it may be that during the course of our testimony issues will arise which should more properly be discussed in executive session.

The Department of State supports this bill because we believe it strikes a correct balance between needs of a free society to maintain a strong foreign intelligence capability and the rights of the citizens and inhabitants of a free society. We also support the bill because it will create a clear statutory basis for the conduct of electronic surveillance for foreign intelligence purposes. As such, the enactment of this bill can do much to help restore the faith of the American public in the intelligence community and in the government as a whole—including the ability of Congress and Executive to work together to protect our liberties and security.

We recognize that there are some risks in this bill. There are risks that it may be interpreted by courts in such a way that we are unable to obtain intelligence information that we think is necessary, but we believe this risk is slight and we believe it is worth taking in order to accomplish the objectives I have already discussed. This bill has the additional advantage of eliminating the risk that the authority to conduct electronic surveillance without a warrant will be abused.

We also note that the bill requires the Executive Branch to meet very high and exacting standards in the certification and application for a warrant. I would like to point out for the record that the executive branch has recently adopted standards nearly identical with the standards proposed in this bill. One of the strong points of the bill is, in my judgment, a codification of these stringent requirements into law.

Finally, I am certain that this Committee appreciates the importance of the foreign intelligence activities that will be conducted under the criteria and procedures of this legislation. These activities form an integral part of our total foreign intelligence effort. They contribute information required to support the processes of formulating and carrying out U.S. foreign policy. I am confident that the information needed for this purpose can be acquired within the terms of this bill without violating the rights of U.S. persons. I am also confident that the committee appreciates the sensitivity of discussing this in detail in open session.

Thank you very much. Mr. Hansell will make a very brief statement after which we will be happy to take your questions.

PREPARED STATEMENT OF HERBERT J. HANSELL, THE LEGAL ADVISER, DEPARTMENT OF STATE

Mr. Chairman and members of the committee, I appreciate this opportunity to participate in your review of S. 1566, and in particular, various legal issues presented by that legislation. Since the Attorney General has testified before you regarding many of those legal issues, I will not attempt to duplicate the matters you discussed with him. However, there are several legal questions that have been raised which have been referred to the Department of State.

Mr. Saunders has expressed the Department's support for the bill. We also want to affirm on behalf of the Department the desire of the Executive branch to work with your Committee and the Congress to achieve a solution of the difficult and complicated issues that are addressed by this legislation.

A question has been raised as to whether this bill should be amended to deal with surveillance activities abroad affecting United States persons. We fully recognize the importance of enactment of legislation establishing authority and standards for such surveillance; but our strong preference would be to deal with that subject in separate legislation, in view of the complex issues presented and the circumstances in which we now find ourselves with regard to the bill that is before you.

We fear that introduction of that subject into this legislation would unduly delay the consideration and enactment of this bill. We are working with the Department of Justice and the members of the staff of this Committee to develop legislation on that subject. I assure you that Secretary Vance and the Department of State are eager to complete the drafting and introduction of such legislation, and will work diligently with you to that end.

It is my understanding that the Attorney General has discussed with you the matter of use or dissemination of information acquired with respect to a United States person who is not a surveillance target. I assume his discussion of the so-called minimization procedures satisfied the desires of the Committee in this regard, and will not go further into that subject matter at this time.

We look forward to discussing with you in Executive Session various other matters and legal issues relative to this legislation.

Mr. Chairman, this concludes the formal presentation by the Department of State. Mr. Saunders and I will be glad to participate with the other witnesses in responding to questions that you or other members of the Subcommittee may have.

Thank you very much.

Any other comments any of you would like to make before we proceed to general questioning?

If not, let me ask a couple of questions here, primarily of the State Department situation. Minimization procedure, referred to on page 8, restricts the distribution and use of information unless that information relates to the ability of the United States to provide for the national defense or security of the Nation, to provide for the conduct of the foreign affairs of the United States. Both of these are quite broad areas. Perhaps the minimization ought to obtain such information as is essentially related to or significantly related to national security or the conduct of foreign affairs.

What I am really wondering here is, how do you interpret particularly the second statement dealing with the State Department, related to the ability of the United States to provide for the conduct of the foreign affairs of the United States? Is that overly broad? Does that give you a blank check to operate? What is your interpretation of that particular statement?

Mr. SAUNDERS. If I may just provide a general answer, it has been and remains difficult to interpret limits of that kind, but just to provide a human analogy for a moment, I think you have to make some basic decisions to begin with about what kind of environment you need to operate in, what kinds of knowledge you need to have to conduct foreign relations. I remember when I was 16 and had to get glasses, my doctor asked me, or I asked my doctor, how long do I have to wear these things, and he said, it depends on how much you want to see, and it is that kind of question that has to be answered first, before you can answer your question.

I think the assumption of the State Department and, I believe, the assumption of this committee is that the United States should have the best intelligence possible within stated limits as a basis for the conduct of foreign relations. In our view, what is essential then to the conduct of foreign relations is what is essential for us to operate with full vision? What is essential for us to operate not in the dark? What is essential for us to operate without denying to ourselves information that is available to other people operating in a global environment? Therefore, we have interpreted the word "essential" in the literal sense of the word, that it is—this knowledge is an essential, an integral part of operating in this kind of environment.

That has been our interpretation, and perhaps it is a bit broad, but we are very conscious, when we sign a certification, of the fact that there are limits in the use of that word, so we do not regard it as a blank check at all. We are very conscious of limits of propriety, sensi-

tivity, or potential damage to foreign relations, and so on, but we do have to accept certain basic assumptions about how we are going to operate in the world and once we are agreed on that, then I think your definition of the word "essential" becomes one that people can agree on.

Perhaps Mr. Hansell would like to add a more precise legal response.

Mr. HANSELL. Well, I think we do need to acknowledge candidly that it is a broad standard, and one that in the drafting process we thought and, I believe, still think would be appropriate. I suppose that in the context of the full bill this is something we might at an appropriate stage want to take another hard look at, but initially on our review of this we felt that although broad, we would prefer to have that flexibility, if it were feasible to do so. Therefore, it was written in this form, but I think we would be prepared to take a hard look at it.

Senator GARN. Well, the reason I asked the question, I think both of you know, not only from this year but last year, I am one who wants to draw that balance, as I have said, and not be too restricted, where we so overly protect the rights of the individual that we are endangering the national security, but even being on that side of the issue, this seems like rather a broad, open-ended standard.

I am not saying that you would misinterpret this point, but again what Senator Hart was saying, who is here now and who is here in the future, and I certainly hope none of us are here forever, Senator Hart. I don't really want to be around that long, even if the people of Utah want me to be, so it is something that I would appreciate if you would take a look at, because it does seem rather broad. I am not questioning anybody's integrity of interpreting it too broadly.

Also, from a State Department standpoint, could you explain to us what sort of obligations are incurred when we as a country license foreign businesses? I am specifically referring to the many hypothetical situations that have been used. We have talked a great deal about airlines in the last 2 years, as well, employees of a foreign airline. What kind of obligations do we incur when we license a foreign business to operate in our country in general terms? I do not want a long legal discourse.

Mr. HANSELL. Well, a great many businesses, of course, can conduct their activities without any license, approval, or permission, whatever, but in the case, for example, of a foreign air carrier, to use the example that was mentioned earlier, there are landing rights and operating rights that would be provided through established processes, and in the case of foreign air carriers, under international agreements. When you say obligations, there would be, of course, under particular international agreements which confer rights or benefits on businesses of a foreign country, obligations that might be imposed by the terms of those agreements or treaties.

Now, however, if you are thinking about obligations in respect of issues that are addressed by this bill, with a few exceptions I think our answer would be, there are not significant obligations that are undertaken that would be impinged upon by this bill or the activities that are dealt with in this bill.

Senator GARN. Ms. Siemer, did you have any desire to comment on the first part of my first question to them about the phrase, "to provide for the national defense or security of the Nation?"

Ms. SIEMER. With respect to minimization procedures, Senator?

Senator GARN. Yes.

Ms. SIEMER. Well, I would point out that there is an important tradeoff here. The minimization procedures under 2521(b)(8) cover all information concerning United States persons. Now, that covers information and the communications of people or entities that are not United States persons. That is a very broad coverage for minimization procedures. So when you trade off the very broad coverage of the minimization procedures against the somewhat more lenient standard that we would apply, that is, "relate to" the ability of the United States "to provide for the national defense," you probably have a fair balance in this bill. We would urge that you give attention to the enormous coverage that you have here instead of only focusing on the kind of standard that we will apply to all of these communications that are covered.

Senator GARN. Well, I appreciate that answer, because I do feel that even asking the questions I am pulling out of context of the whole bill in asking it, so I appreciate your answer, because I agree with you. I think there are other parts of the bill that narrow those definitions sufficiently, at least, for this particular Senator.

Senator Stevenson, you have had no opportunity to ask questions. All of them have made their prepared statements, so anyone that you would like to address your questions to, and I might add that on any of these questions where you are operating as a panel, if you have something you would like to say in addition to what the person to whom the question is addressed, please feel free to let us know so that you can respond.

Senator STEVENSON. Thank you, Mr. Chairman. I think there are two principal causes for public anxiety about electronic surveillance in this legislation, and that anxiety is not unreasonable, in my judgment. The first cause is owing to the inability of the public to perceive the need for surveillance. So, I would hope that you could do more to describe for the public the product as you do for us. We are in a far better position to understand the need than is the public, and based on what we know I do not see any good reason for not doing more than you have done to describe in general terms the product and the national benefit from electronic surveillance in terms of enhanced national security and individual security. That is not a question. That is a most respectful suggestion.

The question I have goes to the second cause of anxiety; and that has to do with the adequacy of the safeguards, trying to strike that balance between the rights to be secure as a nation against our rights as individuals to be secure, and realizing that in this legislation we would rely principally on ex parte and judicial procedure, and being an ex parte procedure, no one can have absolute wholehearted confidence in it.

Now, to provide the public with additional assurances and ourselves as public officials with additional assurances that surveillance will not be used to abuse the rights of American citizens, this committee has in the past worked out with the Justice Department procedures which have assured us as elected representatives of the people access to information about surveillance. Those procedures have been worked out informally, embodied in the law, and they are consequently falli-

ble, and they are subject to change as personalities change. They are, in my judgment, the most effective means there is of guaranteeing that there will not be abuses, and of giving the public greater confidence in this process.

It goes beyond the *ex parte* judicial procedure to actively involve elected representatives of the people in that process.

Now, that is a long question. In the past there have been some difficulties with this procedure because, one, it has not involved our counterpart on the House side. Until now we have had no counterpart on the House side, and there have been, I think, on the part of the Intelligence Community and the Justice Department some reasonable concerns about disclosure and notification on the House side, largely because there hasn't been such a committee as this in that body.

There is now a House Intelligence Committee, or there soon will be. I don't know what the status of the proposal is at the moment. There will be if there isn't already a counterpart for this committee in the House of Representatives. That being the case, everything else having been said, how would you all feel about nailing the kind of procedures that we have all worked out, that we have worked out informally with this Senate body, with the Justice Department, in the statute, in order not only to give the public that *ex parte* judicial procedure, but a statutory assurance that personalities can come and go and the political climate can move around but there is going to be continuing oversight by agencies of the two bodies of the Congress? Also, that oversight is going to include statutory obligation on the part of the appropriate agencies to keep us continuously and fully and currently informed about surveillance?

Mr. LAPHAM. Senator, I think the Director, while he was here, indicated his preference not to see more detailed reporting requirements go into the bill, but rather leave such requirements to be worked out as they have been in the past with this committee and in a counterpart committee that is created in the House. There is, as you know, in draft right now a 12- or 13-page set of procedures which have to do with reporting to this committee the kind of information relevant to the activities covered by this bill.

That procedure has not yet resulted in a full meeting of the minds, I don't think, but such a procedure, I am sure, will be established. I think it is the Director's preference to work through those kinds of letter agreements rather than by legislation, and I take his main reason to be that you may well find over time that you are going to want to change some aspects of these reporting requirements. You are going to want less or more, as the case may be, so it is desirable to have the flexibility that those kinds of arrangements would give, rather than the more inflexible arrangements that legislation would create.

Senator STEVENSON. Well, speaking for one Senator, that is not a satisfactory response. Does it represent the position of the other agencies?

Mr. HANSELL. Senator, may I ask, just to explore a bit some of the parameters of the suggestion, what kind of reporting are you envisioning here? The product of the surveillance would be reported, or simply descriptions of the activities that are undertaken? It is not quite clear to me what you have in mind.

Senator STEVENSON. Well, what I have in mind is a requirement similar to that which is now in S. Res. 400, that would not have to entail pre-notification. It would not except upon request—this is my tentative thinking—have to include the names of specific individuals, but currently, in a timely fashion would require notification to the appropriate agencies of the Congress, and its counterpart, that circumstances have led the agency to seek the order and it has been executed. Also, with sufficient detail to enable us to get back to the agency in such circumstances to seek further information.

In that sort of situation there would be some flexibility. Now, at that point I would agree with Mr. Lapham that on the basic proposition that there will be a timely notification in sufficient detail as to inform us of the circumstances, if not the personalities. I think there should be flexibility, and the public should accept flexibility.

[Pause.]

Mr. HANSELL. Well, I am sure I can speak for the Department of State, and I think for the whole——

Senator STEVENSON. Well, I am sorry to interrupt, but to go one step further, I do not think what I am suggesting as a matter of statute is very different from what is already happening as a matter of informal arrangement and agreement.

Mr. HANSELL. I think we would all share your opening comment, that the concerns and anxieties of the public in regard to the subject matter are not unreasonable. That is, of course, why we are all here. I suppose the question really would be whether a procedure such as the one you outline would in fact serve the objective of public reassurance that the balance is being struck properly. I think it is one that I would not personally want to try to resolve or reach a judgment on the spur of the moment. I can think of some considerations, frankly, that would lead me to think that it would not advance that cause. Therefore, I would want to think about it.

Senator GARN. If the Senator will yield for a moment, I do not think you are as far apart as you appear to be, as I listen. We discussed this at great length last year, primarily in terms of additional specific reporting requirements in detail, besides number of cases, looking at just this particular area of foreign intelligence electronic surveillance, and whether that was necessary or not, the discussion about the raw figures were rather meaningless unless there were some explanation.

I think what we came to last year, Adlai, was under Senate Resolution 400. We have the ability to ask for any further detail that we wanted. We have that legal authority to do so. If I am not mistaken, I do not think the Senator from Illinois is asking for that kind of procedure to be formalized, a lot of detail, and I think he is merely saying that what we worked out in general, that you report and then if we desire further information we can get it. Is that correct, Senator?

Senator STEVENSON. Well, that is correct as far as it goes.

Senator GARN. Well, you are asking for notification statutorily.

Senator STEVENSON. I am asking for it in the law, and perhaps one way of complying with this statutory requirement as opposed to the procedures that have been worked out in the past would be to simply supply these two agencies of the public with the applications to the courts, and you know, the supporting justifications for them. Now, that

would be a procedure which would give us more detail than I had suggested originally. It was a mechanistic matter to make compliance easy.

I had thought that we might be able to give the public their reassurance and in fact prevent any abuses by settling for somewhat less detail than that, but sufficient information to enable us to move if it was indicated.

[Pause.]

Senator STEVENSON. The Senate has already acted on this proposition somewhat generally. It did so when it created this committee. It said:

> It is the sense of the Senate that the head of each department and agency of the United States should keep the Select Committee fully and currently informed with respect to intelligence activities, including any significant anticipated activities, which are the responsibility of or are engaged in by such department or agency, provided that this does not constitute a condition precedent to the implementation of any such anticipated intelligence activity.

It goes on to say:

> It is the sense of the Senate that the head of any department or the United States involved in any intelligence activities should furnish any information or document in the possession, custody, or control of the department or agency or person paid by such department or agency, whenever requested by the Select Committee with respect to any matter within such Committee's jurisdiction.

We would not be here today if this whole subject were not within our jurisdiction.

Ms. SIEMER. Senator, is it your position that that resolution is insufficient for the purposes of reassuring the public?

Senator STEVENSON. Yes.

Ms. SIEMER. In what respect is it insufficient?

Senator STEVENSON. It does not have the effect or the force of law, and of course it does not include the House, and it is general.

Ms. SIEMER. Is it your view——

Senator STEVENSON. And we are considering a law now, and not to put it in the law would be a rather conspicuous omission and would be regarded by some as a retreat.

Ms. SIEMER. Is it your view that the bolstering of the public confidence that is needed, is needed with respect to surveillances of foreign powers as well as United States persons, or that that is limited to United States persons?

Senator STEVENSON. I don't think there is any question but what it goes across the board, but on 90 percent of that board we are already operating, I think, quite effectively. What we are concerned with here is a bill, and we all know what it entails, and if you are suggesting that what I suggested is that the only concern is reassurance to the American public, you are wrong. It is not just to assure the American public that everything is hunky-dory, and then forget about it. It is to assure the American public by making damn certain that there are not going to be any abuses, and it is for that related but twofold reason that I want to see that obligation laid by law on the agencies of the Executive branch, instead of some informal procedure which can be changed, as Mr. Lapham indicated. It can be forgotten or left to some resolution of the Senate which only applies to one House and does not have the force of law.

Ms. SIEMER. No; I was concerned, Senator, and I will explore whether there is a possibility we could arrive at some accommodation of your concern with respect to a notification requirement by including notification with respect to surveillances that affect United States persons, and leaving to the current established, and to my understanding, very effective informal procedures those that are more sensitive, in which the security concerns are enormously important. These are the surveillances of foreign governments in whose communications Americans are never parties and rarely mentioned.

Senator STEVENSON. I personally would, you know, be willing to consider some such differentiation, partly because once we go beyond citizens, it is hard for me at the moment to perceive where you do stop. My principal concern is for the rights of American citizens, and it is those rights that I am seeking to assure will be protected. The other procedures have worked well, and they applied in a variety of different contexts, and might well be used to cover the other part of the situation.

Mr. HANSELL. Why don't we take that under consideration? I think one difference between the procedure as it now exists informally, of course, and what would exist under the statute is the warrant provision, which as a new element brings the judicial branch into the picture, and I think it is worth considering how the three branches of Government will all be involved in one type activity, but why don't we give some thought to it?

Senator STEVENSON. Thank you.

Senator GARN. Senator Hart?

Senator HART. Mr. Saunders, just one question. Under your current procedures and questions, what role does the Secretary of State play in making determinations about electronic surveillance of foreigners?

Mr. SAUNDERS. He is personally very aware of all of the problems that are being addressed in this legislation, and we have discussed the legislation itself extensively with him. Now, coming to the procedures, we do not normally take to him necessarily every single case that may be involved in our Department of that kind. We go to the highest level where we feel that a reasonable position can be arrived at by somebody speaking for the Secretary.

In any case, where there is the slightest question or where there is sensitivity that may particularly involve things that he or the President are concerned about, we err on the side of taking the case to the Secretary, and the procedures normally, routinely would stop short of the Secretary, but only for the routine.

Senator HART. One can make an argument that none of these cases is routine. What factors differentiate between those that stop somewhere short and those that go all the way?

Mr. SAUNDERS. Well, I think what we are involved in here is, when you have a new Secretary of State, he has a maximum opportunity to look at every case and that has been indeed the process that we have engaged in. Once you learn what his views are, [you learn] what he regards as routine and what he regards as the limits within which you may speak for him, and [then] also [you learn] what cases are particularly sensitive in his view and so you take it to him and so he has

been involved in an extensive review of our entire program. We are now beyond that, and when I say routine, I am speaking in terms of my understanding of what in his view would be acceptable limits.

Senator HART. In other words, over a period of time an informal personal policy emerges.

Mr. SAUNDERS. That is right. That would be the case with each new incumbent, I would think.

Senator HART. Is there any element of deniability involved there, that there may be some cases where you do not want the Secretary to have known because if it blows up he can say he didn't know?

Mr. SAUNDERS. Quite the reverse. It seems to me that the principle I have to operate on is that the President and the Secretary cannot be taken by surprise by anything of this kind, so if there is any doubt at all about any aspect of a program, I would consult with him.

Senator HART. So you are able to assure us that under present practices the possibility of a surveillance which has serious foreign policy implications being undertaken without the Secretary's knowledge is for all purposes impossible?

Mr. SAUNDERS. That is right. I regard my vote on the panel that Admiral Turner spoke about as my speaking for the State Department, and I do not take lightly my speaking for the State Department. When I do, I am sure I am speaking for whatever elements of the Department need to be involved in that process, including the Secretary where that is warranted.

Senator HART. Thank you, Mr. Chairman.

Senator GARN. Senator Stevenson, do you have any other questions?

Senator STEVENSON. I will pass, Mr. Chairman.

Senator GARN. I just have one more I would like to ask of Ms. Siemer. On page 2 of your prepared statement, signals intelligence operations covered by this bill do not involve the targeting of individuals. I would like to clarify one point in the bill. The first definition of electronic surveillance reads as follows:

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

As you read this definition, do you believe it would authorize signals intelligence operations involving the targeting of individual U.S. citizens?

Ms. SIEMER. That provision, Senator, is intended to apply in a situation where you have identified a person and know he is a U.S. person, and you know he is in the United States, and then to authorize—not only to authorize surveillance but to include in the definition of electronic surveillance, that kind of activity. This provision is designed to make more precise the definition of electronic surveillance, so that we know what is in it and what is out of it.

Senator GARN. Thank you. Mr. Chairman, I might just state I think we have covered pretty much what we can cover in open session. There are several questions left unanswered, and the necessity of going into executive session exists. All of these witnesses, I am sure, are awaiting and looking forward to an executive session where they can give us

more specific details or information, but with that I will turn it back to you.

Senator BAYH. Well, thank you, Senator Garn. To you and the other members of the committee who were not here when I left, I apologize to you as well as to our witnesses that I had to leave for an hour. Does the Senator from New York have any questions?

Senator MOYNIHAN. Thank you, Mr. Chairman. I must apologize. Senator Hathaway and I were in another such meeting and could not be here.

I wanted to just take this opportunity to ask, and I hope this does not appear to be an ignorant question, of Ms. Siemer, this is the Foreign Intelligence Surveillance Act of 1978. Ms. Siemer, recently, the President in a press conference acknowledged that the Soviet Union is intercepting the telephone calls of American citizens here in Washington and New York, and apparently San Francisco. The Soviet Union is systematically bugging the American citizens and their conversations.

He said that the Defense Department was secure and the White House was secure. He left it at that, and he left it that the rest of us were not, and I wondered, is there any provision regarding this—we assume this is a crime, somebody is committing crimes on a massive scale. Probably in the history of such criminal activity there has never been such a widespread and sustained and sophisticated form of crime. It is a violation of the fourth amendment rights of American citizens.

Does your bill make any such provision—It says, I gather, the United States cannot violate the fourth amendment rights of Americans, but does it say the Soviet Union can or cannot?

Ms. SIEMER. Well, Senator, this is not my bill, but there are two provisions that are important in that regard. One appears on page 28, which is section 4(e)(ii), which permits the Department of Defense and the other intelligence agencies to determine the existence and capability of electronic surveillance equipment being used unlawfully. That is a provision that is very important to us in this regard, and we urge that that provision not be amended.

The second part of your question, I think, would be covered by title III of the Omnibus Crime Act, and should unlawful electronic surveillance ever be discovered in time and in a situation where there was a capability with respect to prosecution, there certainly is a statute that permits the Justice Department to do that. The problem is finding it and finding it in a circumstance where the parties who are doing it can be prosecuted.

Senator MOYNIHAN. That is a very direct answer of the kind we have learned to expect from you in a very admiring way.

Now, the Russians are over on 16th Street bugging our telephones right now. That is against the law but we are not doing anything about it now, but would we do something under the new law?

Ms. SIEMER. Under this law, with respect to the Defense Department's responsibilities, we would continue our activities to determine the existence and capability that the Russians have in that regard, and that information would be made available both to the State Department and to the Justice Department, who have the responsibilities of determining whether——

Senator MOYNIHAN. You would tell us. Now, evidently for the last couple of years the U.S. Government has known that a foreign government has been systematically invading the privacy and violating the fourth amendment rights of American citizens, and our Government has not told us this. We learned about it from the New York Times. The President confirmed it. Was the Government committing a crime when it did not reveal its knowledge of the commission by others of a crime? I am not a lawyer, but isn't there a form of participation when you observe a crime taking place and neither report it nor intervene to prevent it?

Ms. SIEMER. You are referring to misprision of a felony?

Senator MOYNIHAN. Misprision, that is the word. Is there misprision of a felony by the Secretary of Defense?

Ms. SIEMER. No, Senator, I believe there is not.

Senator MOYNIHAN. But would you think that is something the general counsel should decide or a jury should decide?

Ms. SIEMER. Senator, on those matters we defer to the State Department and to the Justice Department with respect to whether——

Senator MOYNIHAN. How do you feel about misprision of a felony with respect to the Secretary of State?

Ms. SIEMER. On that I certainly would defer to Mr. Hansell, since I do not advise the Secretary of State. My job is to keep the Secretary of Defense aware of these kinds of difficulties, and I do not believe that he has any legal problem in that regard, but it is important that the Defense Department defer to the Secretary of State in those instances because it is their province.

Senator MOYNIHAN. I would like to make a point, though. We know that the Soviet Union is committing a crime on a massive scale, a particularly heinous crime, in our view, one which we very much find offensive. A dirty business, we would call. Didn't Holmes call it a dirty business? A dirty business, and here they are doing it to us. We certainly don't want our Government to do it, and our Government shouldn't do it to us, but it is OK if the Communist Government does it? Not being democratic, it is not expected to maintain democratic forms. Is that it? I wonder if the State Department representative would say, the Secretary of State, who knows about this, and his predecessor, who knew about it, are they guilty of a misprision of a felony? Is anybody guilty?

Mr. HANSELL. Senator, I think we will answer——

Senator MOYNIHAN. One question at a time?

Mr. HANSELL [continuing]. That question no.

Senator MOYNIHAN. I'll bet you always say that.

Mr. HANSELL. I can't say that I have been asked the question before.

Senator BAYH. You never had Senator Moynihan before.

Mr. HANSELL. I can't speak with any authority as to what has taken place, what took place with respect to the subject matter prior to this year.

Senator MOYNIHAN. I can tell you. The President told us. Secretary Kissinger knew about it. Secretary Vance knows about it.

Mr. HANSELL. There has been a great deal of work and effort that has been done and is being done with respect to this.

Senator MOYNIHAN. The President said that, too. He said, I have taken care of myself, and the Defense Department has taken care of itself. He said, that is enough.

Mr. HANSELL. But a good deal more. The dollars involved, of course, could run into the billions in terms of responsive, protective measures. There are some limitations. There are some aspects of this that I suspect we could pretty productively discuss in executive session. There is, as I understand it, at least, and has been, though as I say I wouldn't choose to speak of the past—I have not been associated with it—a great deal of effort underway to develop appropriate responses to various facets of the problem.

You are aware, of course, of the diplomatic immunity aspects of the problem.

Senator MOYNIHAN. There is nothing in diplomatic immunity that enables a representative of a foreign power to commit crimes without let or hindrance. What diplomatic immunity provides is that we cannot put them in jail but we can ask them to get the hell out of the country. That is what diplomatic immunity means.

Mr. HANSELL. Well, I guess I would repeat all that I have said thus far.

Senator MOYNIHAN. Yes, sure. I am not trying to press you.

Mr. HANSELL. It is a complex, difficult problem that is engaging and has been engaging a great deal of time on the part of a lot of people, and it is not simple.

Senator MOYNIHAN. Sir, I think I am pressing you beyond the point, and I don't want to keep the Chairman beyond this point. Let me say to you one thing. It is a very difficult problem, and at great expense the U.S. Government is trying to take protective measures for itself in such a way to avoid having to tell the Russians that you are committing a crime on our soil, not just randomly and incidentally, but systematically on a scale never known to technology or history or criminal behavior.

I will say something else to you, sir, to which you do not have to respond. Our government has acted in a pusillanimous manner in this regard. We are sworn, the members of this panel are sworn, the Secretaries of the Departments are sworn to protect the Constitution of the United States against all enemies, foreign and domestic, and we are not doing so. We are letting constitutional rights be systematically trampled on. We are letting the Russians treat us as if we were Russians, not freeborn Americans, and we are doing it out of a fear of offending the principles of detente.

Senator BAYH. With all respect to the Senator, I do not know that he is aware of this, but I must say it is a much more complicated situation. I don't want to interrupt his train of thought here, because I share his concern, but perhaps I should let you answer the question.

Senator MOYNIHAN. May I say, Mr. Chairman, I did not address that question to him, because I think it is not fair. I was stating clearly a judgment to which it would not be fair to ask a representative of the Department to respond.

Mr. LAPHAM. Senator, before you leave the subject, I must cross a legal sword. As much as we would like to think that the fourth amendment applies to the Soviet Union, I do not think the Constitution supports you on that. That amendment, of course, is a restraint on the U.S. Government.

Senator MOYNIHAN. I recognize that fourth amendment rights are only American-given.

Mr. LAPHAM. Yes.

Senator MOYNIHAN. And you are quite correct in saying that the fourth amendment applies to the American Government, but you would agree, would you not, that the Bill of Rights establishes a presumption of what is legal and what is not legal? If you remember the constitutional history of those who opposed the Bill of Rights on the grounds that to list what Government could not do would be to suggest that what was not listed the Government could do, and in the end I think a legally illogical but prudential decision was made to say, let's list these things anyway. You cannot invade privacy, you cannot do thus and such. All right.

I do not say that the Soviet Union is violating our fourth amendment rights. I say they are violating the statutes of the State of New York. I say they are treating Americans, they are treating our citizens the way they treat their citizens, and I say to hell with that. I think it is time we stood up and told them, stop it, and it is the spectacle of the American Government letting the rights of its people be trampled on for fear of incurring the displeasure of the most savage totalitarian government in the history of the 20th century, in the history of mankind, that ought to strike fear into our hearts.

Are we so frightened of the disapproval of the Soviet Union that we will not even protect the rights of American citizens on our own soil? The avoidance of the reality, the fear of revelation, the dismissal by the Administration, saying, well, we have protected the Pentagon and the White House, so what is left to be done—I don't want to press the point, Mr. Chairman. I have already spoken longer than my intention. I know the Chairman is concerned about this. There is not a member of this committee whose concern about transgression by our Government does not extend to transgressions by other governments as well. I think it is important that this legislation will in fact require the Department of Defense to be open about things that previously they may not have been open about or they may not have known about.

I think that is an important provision and yet another reason to support this legislation, which I do, of course, acknowledge as yours, and not only the most recent service you have done this Republic, Mr. Chairman.

Senator BAYH. If you had just started there, I would have been a lot happier. [General laughter.]

I want to say to my colleague, and I have talked to him personally, that we were all concerned and perhaps frightened when we learned what was happening. This committee was informed some time ago about this. It has been going on quite some time before we were, and I think to make certain that we convey perhaps a little greater sensitivity on the part of the administration than could be gathered from the dialog so far——

Senator MOYNIHAN. Diatribe so far, Mr. Chairman.

Senator BAYH. No; dialog, dialog. You are not going to catch me on that one. [General laughter.] I think it is fair to say, is it not, gentlemen and Ms. Siemer, that the administration is really geared up, trying to resolve the problem, and that they are trying to use various techniques to secure a lot more than the White House and the Pentagon. We are very close to the old adage of, he who lives in glass houses theory, as far as how we address ourselves to this problem. I

may have said too much to have said that, but the rest of it perhaps should be dealt with in closed session.

Is there anything further, Senator?

Senator MOYNIHAN. I don't want to cut this off, but I think we are very close—at least I think what I said is very close to as far as I ought to go. Somebody else may care to go further.

Senator BATH. Senator Hathaway?

Senator HATHAWAY. Mr. Chairman, thank you very much. I had one question that I wanted to ask Mr. Saunders in particular, but anybody else could comment on it. I am concerned about the basis for a tap where it is deemed essential to the successful conduct of the foreign affairs of the United States. That seems to me to be fairly broad, and particularly heinous when you are applying it to friendly nations, for example, Canada. I suppose if an airline pilot for Canadian Airlines, which is owned by and run by the country, by Canada, is in the United States, he could be subject to such a tap on the grounds that he has some information that is deemed essential to the successful conduct of the foreign affairs of the United States.

I am even concerned about it when you are talking about that same individual being an agent of a foreign power if the foreign power is the Soviet Union, because it seems to be a very broad basis. I wonder if you can justify it?

Mr. SAUNDERS. Well, before you came in we had a discussion about the way the word "essential" can be interpreted or has to be interpreted. Certainly one of the aspects, going to your first case, one of the aspects that one first takes into account in dealing with the proposal to surveil a particular target is the question of the relationship which the United States has with the nation under consideration at that point.

Certainly we are very aware of the fact that there are some nations who are close to us and who should not be dealt with in that way. That just goes without saying. The sensitivity question is uppermost in our minds.

Senator HATHAWAY. Yes; but you are still not precluded under the law. Even though you as an individual think you shouldn't tap some Canadian, your successor or somebody else might think, "Well, we ought to."

Mr. SAUNDERS. That might be true, but I would suspect that the canons that govern how you conduct your relationships go well beyond the tenure of one particular individual, when the relationship is so large and so important that it would dictate the same kinds of considerations in the obvious cases to one person as to another. What I said——

Senator HATHAWAY. What you said is, as a practical matter, you would not do it. Is that what you are saying?

Mr. SAUNDERS. That is right.

Senator HATHAWAY. Of course, we have the Micronesian situation, where it was actually done, and I think prior to that you would have said you would not do it there.

Mr. SAUNDERS. Well, the State Department did take a position against it.

Senator HATHAWAY. But somebody in the United States Government did it.

Mr. SAUNDERS. I think what you are doing with the passage of this law and with the increased consciousness both here in the Congress and in the Executive branch that is developed by there being such a law suggests that some cases which should not have happened in the past would not happen in the future because they will be the subject of much more intensive review than was the case in the past. The procedures are more airtight now than they were before, I hope.

Senator HATHAWAY. The procedures within the Department, you mean?

Mr. SAUNDERS. Within the Executive branch. I was thinking of the intelligence community at large.

Senator HATHAWAY. Well, would you have any objection if we simply eliminated all friendly countries, for example, or even listed the countries that you say you should be able to tap for this purpose?

Mr. SAUNDERS. I think one gets to the old problem here that it is very difficult to write every case into law, and I think all of us recognize that the President and the Secretary of State need a certain amount of flexibility in the conduct of a program like this. The question is whether or not the Congress is in a position through the knowledge it has to exercise on behalf of the people the appropriate oversight. Writing a list into law, it seems to me, is unduly restrictive. It seems to me that the purpose of doing that can be accomplished in other ways through review procedures in which you participate.

Senator HATHAWAY. But it seems we have an interest, not only in protecting, as Senator Moynihan and others have said, the rights of Americans from being tapped, but certainly the rights of those who are visiting this Nation, particularly from friendly foreign countries, to feel free that they can make telephone calls and not be overheard.

Mr. SAUNDERS. I think the State Department, in general terms, is the organization in the executive branch that is most deeply aware of the damage that is done when something improper is done in the context of a relationship with another country. And we weigh very carefully every time any intelligence operation comes up, the gains from that proposed operation and the risks from its disclosure, and this is the essence of the judgment that we're called on to make.

Ms. SIEMER. Senator, could I add to that; it seems to me that your airline pilot from a friendly nation is covered and does have substantial protection under this bill, because this is the type of surveillance that the Secretary of State could not certify without stating in his certification the basis for his conclusion that the information sought is foreign intelligence information. He must not only state his conclusion that it is, but state the basis, in detail, for his conclusion, and it seems to me that with respect to any friendly power, that basis will be very difficult to state, indeed, if it is not a very special situation. And the Secretary of State is limited by this bill, and that limitation is effective.

Senator HATHAWAY. Well, would you have any objection if we simcessful conduct of the foreign affairs of the United States with respect to Canada, I suppose, would include all the information that we could get about how they feel about the line that we're trying to draw for the fishing limit. Wouldn't that be correct? And there could be, you

know, numerous Canadians that come to this country who might have some information in that regard.

Ms. SIEMER. Well, I think the purpose, Senator, of including the word "necessary" or "essential" is, as Mr. Saunders says, to set not an impossible level or task with respect to that, but indeed—but in fact, a fairly strict standard.

Mr. LAPHAM. Senator, if you're talking about a person, a foreign visitor, somebody who comes to this country and has information of the type you just described, as I understand the bill, any request for surveillance would have to meet the standard of showing that he was involved in clandestine intelligence activities.

Senator HATHAWAY. No.

Mr. LAPHAM. I believe so, sir, at least, that's my understanding of this bill.

Senator HATHAWAY. Not an employee or an officer of a foreign power.

Mr. LAPHAM. You are talking more generally about——

Senator HATHAWAY. No; I am just talking about an officer of a foreign power, and all you would have to show is that the individual has information deemed essential to the successful conduct of foreign affairs. That seems to be a very broad standard.

Mr. LAPHAM. I had not understood your question in the context of employment or the official relationship of that person with his government.

Senator HATHAWAY. Well, now that you understand it, how do you feel about it?

Mr. LAPHAM. I tend to see the standard "deemed essential" as not a loose one, but rather a very tight one. Somebody is going to have to initiate sincere judgment.

Senator HATHAWAY. How do you tell what is essential to the successful conduct of foreign affairs and what is not essential? Can you give me examples on it, or can any of you?

Mr. LAPHAM. I am going to defer to the State Department witnesses on that one, sir.

Senator HATHAWAY. Go back to the fishing example, where at the present time they are trying to negotiate some agreement as to what the fishing rights will be. So I suppose any information that any Canadian had in that regard would be essential to us.

Mr. HANSELL. I don't think you would regard that as essential to the successful conduct of the foreign affairs of the United States, but Senator, I would make another—or two other comments "really" with respect to this. A standard that speaks in terms of identifying friendly or allied countries and nationals of those countries or agents of those countries produces or would produce administrative problems that you want to think through at great length before you would decide how you could write an exception.

There are special circumstances. You know, there are Canadian terrorists, too.

Senator HATHAWAY. I am not talking about terrorism or about that part of the bill. That is fine. That is something that jeopardizes the national security. But here you are talking about something very broad, the conduct of our foreign affairs which could include just

about everything conceivable that relates to our relationship with any country in the world.

Mr. SAUNDERS. I think in the definition of the word "essential" you would be looking to a kind of material that would add a real margin to your knowledge, an additional dimension to your knowledge that would be so important that it would clarify or alter your perception of the problem, and just to cite your example, which is hypothetical, you have the Canadian fisheries. I cannot conceive of an open negotiation like that where the positions would not be so well-known that there is anything that could really be added.

Senator HATHAWAY. Unless you take the Canadian negotiator at GATT. He happens to be in this country, and we are concerned about the tariff on potatoes. He may have in his mind what he is going to bargain for and what he is going to settle for. Wouldn't it be important for us to know just what he is going to put on the table, as to what the tariff ought to be and what he will really take as the bottom line? If he is making a telephone call for that purpose, I think it would be essential for the conduct of our foreign affairs to know that.

Mr. SAUNDERS. I would suspect that given the kind of exchanges between governments like that, that you would be pretty well able to guess what that position might be, and therefore you would judge that the margin that could be added by that kind of operation would not be worth it.

Senator HATHAWAY. I would doubt very much, knowing what our own negotiators do, that we would know just what they had in mind or what they actually would take, without getting information through a wiretap or opening a letter or something like that. They certainly don't put that out on the table. Otherwise, they wouldn't be very good negotiators. So, all I am really getting at is that I think this is way too broad, and I would appreciate it if you would come up with some narrower definition, because I would be in a position right now if we were in mark-up just to move to strike it altogether.

Mr. HANSELL. You are talking, Senator, about the last two lines, lines 24 and 25 on page 25. Is that correct?

Senator HATHAWAY. That is correct.

Mr. HANSELL. Why don't we give some thought to that and see what we would recommend to you?

Senator HATHAWAY. Good. Thank you, very much.

Senator BAYH. Let me ask you to explore a related area. The questions directed by the Senator from Maine in that section of the bill dealt with targeted individuals, where certification has to be made. I am concerned about the fact that although I might accept that standard there, deemed essential, we might differ as to whether that is restrictive or not. Certainly it is more restrictive than related to, yet in the minimization procedures on page 8, where we talk about information that is picked up accidentially, in this area of foreign policy, we are talking about American citizens here, of course, and we do not even use the word "essential." We use the words, "relates to."

Now, shouldn't we use the same standard, or would it cause you problems if we did? I don't want to put words in the mouth of my colleague from Maine, but if he is apprehensive about "essential" he has got to be frightened about "relates to."

Mr. LAPHAM. Senator, I will take a stab at it. There is, as I read the bill, an additional protection in the minimization procedures section requiring that where the information about a U.S. person has to do only with the successful conduct of foreign affairs, that information cannot be maintained in a way such that it is retrievable by that person's name, so that there is that additional safeguard against any possible use of the information in the bill.

Additionally, as a reason to distinguish the one situation, the targeting situation, from the use and dissemination situation, in the one case you are talking about protected fourth amendment rights. You are going to seek to acquire communications of that person. In the other case you have incidentally acquired some information about such a person in the course of conducting a surveillance directed against some other target, and for constitutional reasons I think the reasons for protection in the second case are less than in the first.

Senator BAYH. That might be a good legal argument. It hardly differentiates between damage that can be caused to an individual and the test we ought to apply before we risk that damage. Now, if we are going to get into the whole foreign policy area, which is a very nebulous area, as we know, we have really never done this legally at all, and it is a big step. It seems to me if we are going to risk exposing American citizens in this very nebulous area, hard to define, that we ought to have a high standard. If we are talking about "relates to" protecting the United States against actual or potential attack or other hostile acts of a foreign power, maybe "relates to" is good enough. Or if it is protection against terrorism, maybe "relates to" is good enough there. Or protection against sabotage by foreign power or an agent, and protection against clandestine intelligence activity by an intelligence service of a foreign power, maybe "relates to" is all right there, because you have a pretty good idea of what the definition is. We are talking about a crime there, really, but if we are talking about foreign policy, that is a sort of a fishing net out here.

Besides, I think if you will read carefully, you will find out that what you said is true, but it is true only to information gathered from a person who is a party to the conversation. Senator Hathaway has breakfast at Blair House with the Ambassador or the Prime Minister of Israel or Saudi Arabia, and afterwards he calls—Go ahead.

Mr. LAPHAM. Go ahead, sir. I am sorry.

Senator BAYH. That is all right. Mr. Baron might have the answer, I don't know. Maybe you both had better listen to the question and then have your colloquy.

Senator Hathaway talks to some of his constituents. I don't know how many you have in Maine.

Senator HATHAWAY. Three.

[General laughter.]

Senator BAYH. You talked to the three of them, the Jewish citizens. On the other hand, you may have more than three. You talk to them, and you relate the conversations you had, and then you call Simcha Dinitz down at the Israeli embassy. You could have a conversation with some Arabs and then call Simcha Dinitz.

The minimization procedures that you related to on the top of page 9 and the bottom of page 8 would protect Senator Hathaway if he is a party to that conversation. The way I read that bill, it would not protect him if Dinitz picks up the wire and calls somebody else, picks up the phone and calls somebody else. Hathaway is not a party to that conversation, but Dinitz is relating a conversation that he had. I would assume if Senator Hathaway or Senator Bayh or somebody else is sold on a position and is about to circulate it to a colleague, or to go to the President and urge him to do X, Y, and Z, the President or the Secretary of State might think that that is important but maybe not essential. They might even think it is essential to the conduct of our foreign affairs.

Now, why don't we put "essential" in there instead of "relates to" if we are going to talk about American citizens?

Mr. LAPHAM. I think we have a misunderstanding about what the bill says on that point, Senator, and I need to consult further to clarify my own view, but I understood it to mean that in the situation in which Senator Hathaway might be mentioned in a conversation to which he was not a party that was overheard pursuant to this bill, his name would receive that additional protection which is specified at the top of page 9, namely, his name could not be maintained in a way to make the information retrievable.

Senator BAYH. It says right here, if I might quote, "A United States person without his consent who was a party to the communication." What if he's not a party to the communication, which is the second hypothetical that I raised.

Mr. LAPHAM. Where are you reading, sir?

Senator BAYH. The bottom of page 8, the last three words, the first four words on the top of page 9, "who was a party to a communication."

Mr. LAPHAM. I may have to regroup on that and amend my view.

Senator BAYH. Well, we don't need to have the answer right now, but I think those of us who have been working with this legislation are concerned about that, and I think what we have here is a different standard if someone is a party to the conversation than we have if someone is not a party to the conversation. The information could be the same whether it is out of my lips or somebody in a hearsay situation, it could be just as important to the conduct of foreign affairs, and just as damaging to the individual if it were disclosed.

So I find it difficult to understand why we require essential as far as its impact on foreign affairs in one area and not another. You might run that through channels and study it and get back to us if you would.

Mr. LAPHAM. Yes, sir.

Senator BAYH. Any other questions?

Senator Hathaway?

Thank you very much. We'll look forward to having a chance to try to consummate this.

Admiral?

Admiral INMAN. Senator Bayh, may I add one brief statement. This is my first appearance before the committee. I'm delighted to be here, I look forward to working closely with the committee and it's staff. I'm somewhat concerned from a couple of questions and from

some press treatment yesterday. Let there be no doubt from my examination of my predecessor's stewardship on relieving him on the 5th of July, there are no U.S. citizens now targeted by NSA in the United States or abroad, none. And the procedures in place from the Attorney General are as stringent, as strict and as well complied with in protecting the inadvertent as it conceivably could occur.

And I look forward in executive session in exploring that with as much detail as the committee might ever want to do.

Senator BAYH. Yes, well, I stayed until close to the end but then had to go to another mission, so I don't know what happened afterwards. I don't recall myself or anybody else inferring that American citizens were being targeted by NSA, but if that came out in the news, I am glad you set the record straight.

And Admiral, we will look forward to working with you, sir.

Senator HATHAWAY. Mr. Chairman, may I make a comment before we leave?

There is a story that many in the audience might have heard about. When Robert Benchley was in college, he didn't study very hard, and he came into a Government examination not having studied too hard, and the first question was to explain the North Atlantic Fisheries Treaty of some year, and not knowing anything about it he said, "Well, I think I'll explain it from the point of view of the fish."

I think that one of the shortcomings of this entire bill is that it should have been drafted from the point of view of the person who is being tapped, and if that had been done I think we would have come up with a much better bill.

And those who are here and those who testified earlier should review it again with that in mind, because what we are really trying to do is safeguard the individual, particularly the American citizen, and even agents of foreign powers to a certain extent.

Senator BAYH. Well, I just want to say as somebody who has been very intimately involved in this, I thought the major thrust of this legislation was designed to do what the Senator from Maine thinks we should do, and I share a very common concern about individuals. We have a rather difficult line to walk here, on one side of which we have a responsibility to protect the rights of American citizens as individuals, and also to protect them collectively as a nation. And it is a test that I think we can pass, but as we are trying to deal with the nuances and the sophisticated mechanisms in which those of you who have been kind to be with us this morning are carrying out your charge, we have an equal if not greater responsibility to see that you use those tools and discharge your responsibility in such a way that it doesn't infringe on those who you are protecting collectively.

And I just want to say, as one person who has been involved in this, we, some of us, have been very sensitive to that.

The Senator from Maine is one who is a leader in this and I appreciate his particular concern. I'm glad he's on the committee, frankly.

Do you have any disavowals or any savings clauses you want to slip in before we go into executive session the next time?

If not, if you would pursue some of these things we have discussed and be ready to go at it again, we would appreciate it very much.

[Whereupon, at 12:12 p.m., the subcommittee recessed subject to the call of the Chair.]

WEDNESDAY, FEBRUARY 8, 1978

U.S. SENATE,
SUBCOMMITTEE ON INTELLIGENCE
AND THE RIGHTS OF AMERICANS
OF THE SELECT COMMITTEE ON INTELLIGENCE,
Washington, D.C.

The committee met, pursuant to notice, at 10:22 a.m., in room 6226, Dirksen Senate Office Building, Senator Birch Bayh (chairman of the committee) presiding.

Present: Senators Bayh (presiding), Huddleston, Case, and Lugar.

Also present: William G. Miller, staff director; Audrey Hatry, clerk of the committee.

The CHAIRMAN. The committee will come to order. Members of the committee, distinguished witnesses, let me just take a few minutes to put in perspective where we are, by looking at where we have been, so we will know we are going.

We resume, today, the hearings on S. 1566, the Foreign Intelligence Shattuck and Mr. Jerry Berman, of the American Civil Liberties November 15 last year, and referred to this committee. Our hearings on this bill began last July with testimony from administration officials. We postponed testimony from expert witnesses and representatives of interested groups so they could address the bill as amended by the Judiciary Committee.

We have two panels this morning. The first includes Mr. John Shattuck and Mr. Jerry Berman, of the American Civil Liberties Union, and Dr. Morton Halperin, of the Center for National Security Studies. The second panel will include Mr. Steven Rosenfeld, of the Association of the Bar of the City of New York, and Mr. David Watters, of the American Privacy Foundation, and in absentia, Dr. Christopher Pyle, of Mount Holyoke College, who is at this time somewhere in a snowdrift in Massachusetts. We will all look forward to having Dr. Pyle's prepared statement submitted in the record.

[The prepared statement of Dr. Christopher H. Pyle follows:]

PREPARED STATEMENT OF PROF. CHRISTOPHER H. PYLE, MOUNT HOLYOKE COLLEGE

Mr. Chairman: I am pleased to have the opportunity to testify today. The subject of these hearings has long been of interest to me, as a teacher of constitutional law, as a consultant to Senator Ervin's Subcommitte on Constitutional Rights, and Senator Church's Intelligence Committee, and as a captain in Army Intelligence.

I was first confronted with the problem that faces this Committee ten years ago when, as an officer on the faculty of the Army Intelligence School. I had occasion to take a book down from my office shelf. Inside the cover was the faded imprint of a rubber stamp, which read:

> "This publication is included in the counter-intelligence corps school library for research purposes only. Its presence on the library shelf does not indicate that the views expressed in the publication represent the policies or opinions of the Counter-Intelligence Corps or the military establishment."

The book was the Constitution of the United States.

Over the years, I have reflected on the significance, and the symbolism, of that disclaimer. The men who stamped it there did not intend to disassociate themselves from the Constitution they had sworn to uphold; they had no strong feelings about the Constitution one way or the other. They simply responded—in an essentially mindless way—to pressures placed upon them by an outspoken Member of Congress who, in his zeal to ferret out Communism, sent his staff out to purge military libraries of "subversive" writings. . . .

Today, of course, the situation is different. Congress is pressing the Executive branch to erase those disclaimers and I, for one, am glad of it. Yet I fear that Congress may achieve little more than cosmetic reform—new rubber stamps proclaiming fealty to the Constitution in place of the old ones disclaiming it—while the same, essentially mindless behavior continues.

The gist of what I have to say today is that despite all of the effort that has gone into this bill, it may achieve little more than cosmetic reform. Indeed, it could be worse. It could turn into a "backdoor charter" authorizing many of the surveillance excesses Congress has so recently deplored.

PSEUDO-WARRANTS

The most disturbing aspect of the bill to me is its disregard for Fourth Amendment principles. The bill purports to extend traditional warrant procedures to foreign intelligence taps, bugs, and microwave intercepts, but, in fact, it does no such thing. Rather, it invents two new "pseudo-warrants," unlike anything the American judicial system has ever seen.

Probable cause to believe that a crime has been, is being, or is about to be committed is the *sine qua non* of a judicial search warrant. The Supreme Court has consistently condemned searches and seizures made without a search warrant, subject only to a few "jealously and carefully drawn" exceptions. E.g. *Schneckloth* v. *Bustamonte*, 412 U.S. 218, 219 (1973) (dictum); *Coolidge* v. *New Hampshire*, 403 U.S. 443, 454–455, 478–482 (1971); *Vale* v. *Louisiana*, 399 U.S. 30, 34–35 (1970); *Chimel* v. *California*, 395 U.S. 752, 762 (1969); *Mancusi* v. *DeForte*, 392 U.S. 364 (1968); *Katz* v. *United States*, 389 U.S. 347, 356–57 (1967).

The only occasion on which a judge may issue a search warrant in the absence of probable cause is when a person refuses to comply with a reasonable inspection request by a public health, housing or fire inspector. E.g. *Camara* v. *Municipal Court*, 387 U.S. 523 (1967) and *See* v. *Seattle*, 387 U.S. 541 (1967). In these instances direct *advance notice* to the subject of the search mitigates the invasion of privacy.[1]

Moreover, the Court orders required in *Camara* are really not search warrants at all, but "certificates of need" legitimizing inspections and lending the contempt powers of judges to inspectors to hasten their entry. The fact that the Court has mislabelled these orders is no reason for Congress now to compound the error. Let there be no mistake about it: the "certificates of need" proposed in this bill cannot be called warrants without doing irreparable harm to the 200-year-old definition of a search warrants. *Entick* v. *Carrington*, 2. Wils. K.B. 291 (1765), *Leach* v. *Three of the King's Messengers*, 19 How. St. Tri. 1001, 1027 (1765); oral argument of James Otis, Jr., in *Petition of Lechmere* (the Writs of Assistance Case). 2 *Legal Papers* of John Adams 139–144 (Wroth & Zobel ed., 1965), and U.S. Constitution. Amendment IV. If this Committee does nothing else to revise this bill, it should at least practice truth-in-labelling and replace the term "warrant" wherever it appears with the more accurate term "certificate of need." Then no one can accuse Congress of perpetrating a hoax on the American people and the departure from Fourth Amendment standards will be plain for all to see.

One need not imagine how the certificates will be worded if the bill passes. John Mitchell's affidavit explaining the need for warrantless taps against the Jewish Defense League provides a perfect example:

---

[1] A generalized form of notice likewise mitigates warrantless searches of persons and objects entering the United States, of places licensed to sell firearms and liquor, and of vehicles for license, registration, and safety checks. E.g., *Almeida-Sanchez* v. *United States*, 413 U.S. 266 (1973); *United States* v. *Biswell*, 406 U.S. 311 (1972); *Harris* v. *United States*, 390 U.S. 234 (1968), as interpreted by *Cady* v. *Dombroski*, 413 U.S. 433, 444–445 (1973). Notice, both general and direct is also present where warrantless welfare inspections are allowed. *Wyman* v. *James*, 400 U.S. 309 (1971).

> The surveillance of this telephone installation was authorized by the President of the United States acting through the Attorney General, in the exercise of his authority relating to the nation's foreign affairs and was deemed essential to protect this nation and its citizens against hostile acts of a foreign power and to obtain intelligence information deemed essential to the security of the United States.

Quoted in Foreign Intelligence Surveillance Act of 1976, S. Rep. No. 94–1035, 94th Cong., 2d Sess. (1976) at 136.

In short, anyone who believes that the certification procedures in this bill will protect liberty must believe that we will never again have an Attorney General like Prisoner No. 24171–157.

READING THE FOURTH AMENDMENT

I know of only one way to bring non-probable cause search warrants under the Fourth Amendment, and that is to read the two clauses of that Amendment separately, as Professor Telford Taylor once proposed. Taylor, *Two Studies in Constitutional Interpretation at* 79–93 (1969). By reading the second clause prescribing warrants as applying to searches for tangible things only, it is possible to treat wiretap warrants as if they were not warrants at all, but mere "surveillance orders" subject only to the reasonableness requirement of the Amendment's first clause. Thus, like searches incident to lawful arrests, and street corner frisks for weapons, wiretapping and bugging could be authorized on less than probable cause.

Whatever the merits of this idea might have been, say, in the wake of *United States* v. *Rabinowitz*, 339 U.S. 56 (1950), time has passed it by. During the past twenty years, the Supreme Court has increasingly read the two clauses together where planned searches are concerned.[2] In *Silverman* v. *United States*, 365 U.S. 505 (1961), the Court held that the taking of information by an electronic bug constituted a search and seizure within the meaning of the Fourth Amendment and its warrant clause. In *Katz* v. *United States*, 389 U.S. 347 (1967), the Court declared that the mere existence of probable cause was not enough to justify the bug; a formal warrant had to be obtained. The *Rabinowitz* theory granting independent potency of the reasonableness clause was specifically rejected in *Chimel* v. *California*, 395 U.S. 752 (1969), and in *United States* v. *U.S. District Court*, the Court took pains to emphasize that "the definition of 'reasonableness' turns, at least in part, on the more specific commands of the warrant clause," 407 U.S. 297, 315 (1972).[3] Congress committed itself to the same principle by passing title III of the Omnibus Crime Control and Safe Streets Act of 1968. See 18 U.S.C. Sec. 2518, and S. Rep. No. 1097, 90th Cong., 2d Sess. (1968) at 94.

A NATIONAL SECURITY EXCEPTION TO THE FOURTH AMENDMENT?

Today Congress is faced with the question, not resolved in *Katz*, *Keith*, or Title III, of whether electronic surveillance to collect foreign intelligence and national security information is constitutionally distinguishable from electronic surveillance to gather evidence of a crime.

The Nixon administration claimed that the president's prerogatives as commander-in-chief and as the principal officer in the conduct of foreign affairs gave him absolute discretion to employ electronic surveillance to collect both domestic and foreign intelligence. Nixon's Justice Department insisted that neither the Fourth Amendment nor Congress could restrain him in the use of "his" surveillance forces. Gov'ts Answer of Def.'s Motion for Disclosure of Electronic Surveillance, *United States* v. *Dellinger*, No. 69 Cr. 180 (N.D. Ill., Feb. 20, 1970).

A chilling record of intelligence abuses persuaded the Ford administration to cease claiming immunity from legislation even as it sought to persuade Congress that it must give statutory recognition to the idea of inherent Presidential powers. Attorney General Levi insisted that a national security wiretapping law

---

[2] Of course, the Court still reads the clauses separately where searches associated with arrest and routine inspections are concerned. *United States* v. *Watson*, 423 U.S. 411 (1976); *United States* v. *Martinez-Fuertes*, 428 U.S. 543 (1976).

[3] *Rabinowitz* retains full vitality only in the area of searches incident to valid arrests. *United States* v. *Watson*, 423 U.S. 411 (1976). Where health, safety, and roving border inspections are conducted, "area warrants" may be required. *Camara* v. *Municipal Court*, 387 U.S. 523 (1967); *Almeida-Sanchez* v. *United States*, 413 U.S. 266 (1973).

could be drafted without reference to the Fourth Amendment because a "national security exception" to the Fourth Amendment had already been established by the lower courts. Hearings Before the Select Committee to Study Governmental Organization With Respect to Intelligence Activities, 94th Cong., 1st Sess. (1975), Vol. 5 at 81–82 (hereinafter the Church Committee Hearings).

To its credit, the Carter administration has dropped Levi's demands for legislation acknowledging inherent surveillance powers. However, the new administration does maintain that a national security exception to the Fourth Amendment exists, and thereby asserts that Congress may write this bill on a clean slate. *Foreign Intelligence Surveillance Act of 1977*. Hearings Before the Subcommittee on Criminal Laws and Procedures. Committee on the Judiciary, U.S. Senate, 95th Cong., 1st Sess. (1977), p. 26.

In my opinion, Congress cannot write this bill on a clean slate, free from the limitations of the Fourth Amendment. To do so would be to adopt the dangerous assumption that where national security and foreign intelligence are concerned, the fundamental principles of limited government, guaranteed liberties, and checks and balances do not apply.

Nothing in the text of the Fourth Amendment, the history which gave rise to its adoption, or the general principles which have evolved since, supports such a view. The fundamental principle, to which all nine Justices agreed in *Abel* v. *United States*, 362 U.S. 217 (1960), is that the Fourth Amendment's protection extends to all people within the United States—even alleged spies who enter the country illegally.

To my knowledge, only one Supreme Court Justice has ever suggested that there might be a national security exception to the Fourth Amendment. That was Justice White who, concurring separately in *Katz* v. *United States*, said: "We should not require the warrant procedure and the magistrate's judgment if the President . . . or the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable." 389 U.S. 347, 364 (1967). In White's view there could be an absolute national security exception to the entire Fourth Amendment provided that the President or the Attorney General personally decides that the surveillance was reasonable.

The Supreme Court refused to adopt White's position in *United States* v. *U.S. District Court*, despite urging from the Justice Department. Gov't's Brief at 11. On the contrary, Justice Powell's opinion for the majority held that both clauses of the Fourth Amendment, with their attendant judicial supervision, apply to national security taps and bugs. Having said this, Powell went on to imply that the Court might be willing to accept Congressional legislation that provided for a "reasonable" system of judicial warrants based on less than probable cause, 407 U.S. 297 (1972) (popularly known as the *Keith* case).

In *United States* v. *Butenko*, the Third Circuit Court of Appeals ignored the holding in *Keith* and judicially decreed a national security exception to the warrant clause. 494 F. 2d 593 (3rd Cir. 1974), *cert. denied, sub nom Ivanov* v. *U.S.*, 419 U.S. 881 (1974). However, that court did not hold that judicial review under the reasonableness clause was not required. Rather, it piously declared: "The opportunity for post search reviews represents an important safeguard of Fourth Amendment rights and should deter abuses that might be caused by the necessary relaxation of the warrant requirement." Id. at 606.

The Supreme Court has been far more concerned about "hindsight coloring the evaluation of the reasonableness of a search or seizure." *United States* v. *Martinez-Fuerte*, 428 U.S. 543, 565 (1976). As the Court observed in *Beck* v. *Ohio*, 379 U.S. 89, 96 (1964), omission of prior warrants "by-passes the safeguards provided by an objective predetermination of probable cause and substitutes instead the far less reliable procedure of an after-the-event justification for the . . . search, too likely to be subtly influenced by the familiar shortcomings of hindsight." The constitutional requirement of prior judicial review was reemphasized in *United States* v. *U.S. District Court*, 407 U.S. 297, 317–318 (1972), where the Supreme Court declared: "The independent check upon executive discretion is not satisfied, * * * by 'extremely limited post-surveillance judicial review.' Indeed, post-surveillance review where intelligence surveillance is involved would never reach the surveillances which failed to result in prosecution." See also *Katz* v. *United States*, 389 U.S. 347, 358 (1967), and *United States* v. *Watson*, 423 U.S. 411, 455–456, n. 22 (1976) (Marshall J., dissenting). In light of these clear statements of principle by the Supreme Court, I find it difficult to accord any precedential value to the Third Circuit's opinion in *Butenko*.

Moreover, the Justice Department misreads *Butenko* when it argues, as it did before the Church Committee, that the decision may be interpreted as a broad statement of law. Church Committee Hearings, Vol. 5 at 81. The *Butenko* court carefully confined its decision to "the circumstances of this case," in which an American and a Russian were convicted of espionage. So limited, *Butenko* is no precedent for the sweeping power to collect economic and political intelligence sought in this bill.

In *United States* v. *Brown*, the other case cited by Attorney General Levi, the Fifth Circuit Court of Appeals did not declare a national security exception to the entire Fourth Amendment, thereby obviating the need for any judicial scrutiny. It merely reiterated its holding in *United States* v. *Clay*, 430 F. 2d 165, 170–172, *rev'd on other grounds*, 403 U.S. 691 (1971), that the President has a surveillance power "over and above the Warrant Clause of the Fourth Amendment." [4] That power, it said, is based on "the President's constitutional duty, in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs." 484 F. 2d 418, 426.

In his seminal lecture "Towards Neutral Principles of Constitutional Law," Prof. Herbert Wechsler wrote: "(T)he main constitment of the judicial process is precisely that it must be genuinely principled, resting with respect to every step on analysis and reasons quite transcending the immediate result that is achieved." It must employ "criteria that can be framed and tested as an exercise for reason and not merely as an act of willfulness or will." Wechsler, *Principles, Politics, and Fundamental Law* at 21, 16 (1961). By Wechsler's standard, the decisions in *Brown* and *Butenko* are no more than naked exercises of judicial will. None of the cases cited in them supports the holding they proposed; nor does either opinion examine the scope of the Fourth Amendment or offer any explanation of why wiretapping for foreign intelligence purposes should not require a warrant.

Viewed together, *Brown*, *Butenko*, and *Keith* indicate a judicial disposition to approve a narrow exception to the warrant clause only. *Butenko* and *Brown* suggest that all elements of the warrant clause may be ignored where foreign intelligence or national security taps and bugs are concerned. Justice Powell's dicta in *Keith* is less expansive; it suggests merely that Congress might constitutionally tinker with some of the elements, such as probable cause, set forth in Title III. 407 U.S. at 308.[5]

DOUBLE STANDARDS

Brown, *Butenko*, and *Keith* all call for a constitutional double standard. In *Brown*, the court holds that "domestic security" taps and bugs come under the warrant clause but those seeking "foreign intelligence" do not. In *Butenko*, the court ruled that the surveillance clearly would have been "illegal" had the subjects of the warrantless taps been "members of a domestic political organization," but since they were suspected of the extraordinary crime of espionage, the warrant clause did not apply. 494 F. 2d at 606. In *Keith* the proposed double standard would distinguish between "the surveillance of 'ordinary crime,'" which would be governed by the Fourth Amendment, and "(t)he gathering of security intelligence" and "domestic intelligence," which would not. 407 U.S. at 322 (1972). Thus all three cases evidence confusion as to the scope of the so-called "national security exception."

As a matter of raw power, I have no doubt that the courts could decree any exceptions to the Fourth Amendment they wish. What I do not understand is the conceptual basis for the distinctions they draw. Nor, frankly, do I under-

---

[4] *U.S.* v. *Clay*, like *Butenko*, held that post-judicial review under the Fourth Amendment's reasonableness clause was still constitutionally required. 430 F. 2d at 171.

[5] Much has been made of the fact that the Court in *Keith* reserved judgment in the question of foreign intelligence taps and bugs. This reservation, and the denials of certiorari in *Butenko* and *Brown*, are taken by some as evidence that the Court, if driven to it, grant a far more sweeping exception to the Fourth Amendment than is advocated in this bill. Against this political judgment, it is worth contrasting the fears of at least one Assistant Attorney General. In an interoffice memorandum to Attorney General Richardson, Robert G. Dixon wrote:

"Although it is true that the Court specifically reserved the foreign intelligence issue, at no point did it volunteer any reasons why it might be willing to make this distinction when presented with a proper case. To the contrary the reasoning in *Keith* seems to anticipate and reject the arguments the Department is making at this time in the lower courts." *Warrantless Wiretapping and Electronic Surveillance*, Joint Hearings Before Subcommittee of the Committee on Judiciary and Foreign Relations, U.S. Senate, 93rd Cong., 2d Sess. (1974) at 35.

stand the basis for the distinction which S. 1566 draws between national security and foreign intelligence surveillance on the one hand, and law enforcement surveillance on the other.

Why should intelligence surveillance be treated differently from law enforcement surveillance? Both are equally intrusive. Both breach the same values that the Fourth Amendment was designed to protect. What theory can justify a finding that the Fourth Amendment bars warrantless searches for evidence of the most heinous crimes, but does not bar such searches where economic or foreign policy information is sought? Can it truly be said that each of the many purposes (disclosed and undisclosed) for which the intelligence agencies seek surveillance powers under this bill is more compelling, or even as compelling, as the need to investigate felonies? *

The government's main argument in support of a constitutional distinction is that where intelligence surveillance is concerned, its intentions are benign. Because its intentions are benign, the probable cause standard may be ignored.

After twenty years of intelligence abuses—FBI dirty tricks, CIA drug tests, and White House "horrors"—it takes nerve to make such a claim. Or perhaps it is just naiveté: the kind of well-meaning naiveté that impels each generation of official housecleaners to assure Congress that their good intentions alone will cleanse the bureaucracy of all evil and banish wrongdoing forever.

According to Attorney General Levi, good intentions on the part of his transient staff were sufficient to transform the Fourth Amendment from a staunch barrier against official intrusion into a shell of its former self. When the purpose of a surveillance is to obtain evidence of a crime, Levi told the Church Committee, the Fourth Amendment has its greatest clout, but where the purpose is mainly to gather intelligence (and only "incidentally" to put criminals behind bars), the Amendment has little vitality and can be easily overridden by unsubstantiated assertions of a national security need. (Hearings, Vol. 5 to 73.)

We have come a long way from the "inalienable rights" of the common law when an Attorney General as learned as Mr. Levi can make such a claim. Clearly ours is an age of moral relativism, in which few rights are absolute and "compelling" state interests may "override" individual rights. But even if the "privacies of life" extolled by the Supreme Court in *Boyd* v. *United States*, 116 U.S. 616, 630 (1886), are not as "sacred" as they once were, it would be wrong to value them as lightly as Levi did. As Justice White observed in his opinion for the Court in *Camara* v. *Municipal Court*, "It is surely anomalous to say that the individual is fully protected by the Fourth Amendment only when the individual is suspected of criminal behavior." 387 U.S. 523, 530 (1967).

Yet S. 1566 devalues the Fourth Amendment about as far as one can go. At the legislative level, the bill assigns minimum weight to the right to be let alone and maximum weight to unsubstantiated claims of official need. At the judicial level, the weighting of the scales is no different: minimum weight to the privacy; maximum weight to unsubstantiated certificates of need.

Before Congress strikes its final balance, I hope that it will accord greater weight to privacy and discount the government's unsubstantiated claims with a healthy dose of Madisonian skepticism. Moreover, I hope that this Committee will lead the way by expressing willingness to sacrifice some governmental efficiency, even in the national security and foreign policy arenas, for the sake of liberty. In this area, at least, it is time to drop our Tory faith in the inherent goodness of government and return to the Whig view that the worth of any government is to be measured by the degree to which it accepts additional burdens so that the people may be left alone.

. . . . . THE BURDEN OF PROOF

On many issues Congress may, like the courts, properly defer to the expertise of the executive. This deference may even go so far as to shift the burden of persuasion to the opponents of certain government-sponsored measures. However, where individual liberties are at stake, no deference should be indulged. When, as here, the agencies backing the bill have been guilty of gross violations of

* *United States* v. *Ehrlichman* adds still another double standard to the list. There the District Court held that the so-called national security exception had been "carefully limited to the issue of wire-tapping, a relatively non-intrusive search." 376 F. Supp. 29, 33 (D.D.C. 1974). But if the exception is valid, why should it be limited to any one technique? The distinction smacks of John Ehrlichman's argument before the Watergate committee—burglaries for the sake of national security are constitutional; murders are not.

liberty and law, they should have to overcome a presumption that their bill is unconstitutional. What Lord Acton wrote to Bishop Creighton should have special meaning to us today: "I cannot accept your canon that we are to judge Pope and King unlike other men, with a favourable presumption that they did no wrong. If there is any presumption it is the other way against the holders of power, increasing as the power increases." J. Acton, *Essays on Freedom and Power* 364 (H. Finer ed. 1948).

If Congress is reluctant to go that far (out of courtesy to the men with the new brooms), then it should at least place both the burden of coming forward and the burden of persuasion squarely on the agencies.

THE PROPOSED NON-CRIMINAL STANDARD FOR ISSUING PSEUDO-WARRANTS

The most extraordinary aspect of the debate over this bill has been the deference which Congress has given to the FBI's demand for broad powers to wiretap and bug persons unsuspected of criminal activity. I find this deference extraordinary because both the Secretary of Defense and the director of the Central Intelligence Agency have admitted that their agencies do not need such powers. Hearings on S. 1566 Before the Subcommittee on Intelligence and the Rights of Americans, Select Committee on Intelligence, U.S. Senate, 95th Cong., 1st Sess., July 21, 1977 (to be published) at ——. No one seems to have asked the Administration to explain why the FBI needs these powers but the CIA and military intelligence do not. I would have thought it would be the other way around; that the foreign and military intelligence agencies would want the power to collect positive intelligence and stem leaks, while the FBI, still recovering from its excessive indulgence in domestic intelligence work, would be content to return to the traditional criminal standard of the Fourth Amendment.

Second, the arguments advanced on behalf of the non-criminal standard are so weak as to seem contrived. Of the six hypothetical cases advanced by the Justice Department, not one is drawn from the realm of positive intelligence. *Foreign Intelligence Surveillance Act of 1977*. Hearings Before the Subcommittee on Criminal Laws and Procedures, Committee on the Judiciary, U.S. Senate, 95th Cong., 1st Sess. (1977), pp. 8–10. Yet, as I shall explain later in this statement, the chief beneficiaries of this bill would not be the spy chasers, but the collectors of positive intelligence. Certainly that must have been the Ford Administration's original intent. S. 1566 is not "The Counterintelligence Act of 1977"; it is the "Foreign Intelligence Act of 1977." If the Justice Department's hypotheticals are truly representative of the government's needs, then the bill should be relabeled.

The American Civil Liberties Union has analyzed the Justice Department's six hypotheticals and finds them unpersuasive. *Id.*, Part II, Appendix to the Minority View of Senator James Abourezk. I agree, but for different reasons.

Hypothetical No. 1.—The first hypothetical attempts to state an instance of industrial spying that does not technically violate the laws against espionage:

> A [reliable] 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 could have a variety of uses including possible use in a sophisticated weapons systems, 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.

The Justice Department argues that "Stealing IBM trade secrets and research and transmitting this material to a foreign intelligence service is probably not a violation of espionage laws," citing 18 U.S.C. Sections 793 and 794. The ACLU argues that it is. Their dispute turns on the scope of the terms "national defense information" and "information relating to national defense," both found in Section 794. The ACLU argues that electronic surveillance of "A" would be lawful under a traditional criminal warrant because the Supreme Court in *Gorin* v. *United States*, 312 U.S. 19, 28 (1941) defined "national defense" as 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." The Justice Department reads that term more narrowly, presumably because its indeterminate language is vulnerable to being declared unconstitutionally "void for vagueness."

I agree with the Justice Department. In *Gorin*, the Court held that the Espionage Acts were designed only to protect "secrets," and in *Heine* v. *United States*, 151 F. 2d 813 (2d Cir. 1945), *cert. denied*, 328 U.S. 833 (1946), a distinguished Court of Appeals held that information cannot be "secret" unless the government takes affirmative steps to designate it as such and prevent its dissemination.

But I do not agree with the Justice Department's effort to get around the *Heine* decision by having a non-criminal standard for pseudo-warrants written into this bill. Given the importance which the Department assigns to industrial spying, it is worth examining the *Heine* case in some detail. Edmund C. Heine was a German-born, naturalized citizen who was employed by the Volkswagen company on the eve of World War II to make confidential reports on the American aircraft industry. Heine collected his information from magazines, books, newspapers, technical catalogues, handbooks and journals. He also corresponded with airplane manufacturers, talked with one or two workers in airplane factories, and questioned attendants at aircraft exhibits at the 1940 New York World's Fair. In talking with people in the aircraft industry, he used a "cover story" to misrepresent his purposes and when his reports were completed he sent them, not to Volkswagen directly, but to "cut-outs" in New York City and Lima, Peru. But since he never stole *classified* information the charge of espionage was dismissed. If a criminal standard for the issuance of pseudo-warrants is adopted, the Justice Department argues pursuasively, future spies like Heine also will go free.

I agree with the courts; future Heines ought to be free of electronic surveillance until they conspire to steal classified information. The ACLU argues for an impermissibly indeterminate criminal law; the Justice Department assumes, as Judge Learned Hand put it so well in the *Heine* case, "that there are some kinds of information 'relating to the national defense' which must not be given to a friendly power, not even an ally, no matter how innocent, or even commendable the purpose of the sender may be." [7] Writing for a unanimous panel Judge Hand added with characteristic understatement, "Obviously, so drastic a repression of the free exchange of information it is wise carefully to scrutinize, lest extravagant and absurd consequences result." 151 F. 2d at 815.[8]

I find the Justice Department's first hypothetical disingenuous because the Department's solution—the non-criminal standard—goes far beyond the problem. Under the sweeping language of S. 1566, any American who confidentially advises a foreign corporation on a variety of non-military matters could be tapped or bugged not because he is engaged in a nefarious scheme, but because the corporation which he advises is, unknown to him, a "proprietary" front for a foreign intelligence service.

Two provisions of Section 2521's definition of an "agent of a foreign power" made this possible. First under Section 2521 (b)(2)(B)(i), the confidential reports can be viewed as "clandestine intelligence activities for or on behalf of a foreign power, which . . . will involve a violation of the criminal statutes of the United States." This is possible because the term "clandestine intelligence activities" is not defined and the "will involve" clause permits highly speculative judgments. The predicted violation of the criminal laws that the government suspects "will" occur may be no more than a technical violation of the extremely vague Foreign Agents Registration Acts, 18 U.S.C. Sec. 951 and 22 U.S.C. Secs. 612, 613, 614(a), 615, 617, and 618(a), or of the equally vague criminal provisions of the Export Administration Act. 50 U.S.C. App. Sec. 2401–2413.

Second, a pseudo-warrant for a Heine-type investigation could issue under Sec. 2521(b)(2)(B)(iii). That provision, if read as disingenuously as Attorney General Jackson read section 605 of the Federal Communications Act, would permit easy surveillance of a person who collects or transmits information not knowing that the request for it came "pursuant to the direction of an intelligence service or intelligence network of a foreign power." Mere unwitting compliance could

---

[7] The Justice Department's hypothetical imagines that the spy it wants to wiretap works for a Soviet block intelligence service, but the statutory language it advances would cover spies of all nations.

[8] One "extravagant and absurd consequence" of this kind of reasoning took place last fall when officials of the National Security Agency cast about for some way to suppress publication at international conferences and in academic journals of new developments in theoretical mathematics which could give all governments secure cryptographical systems. For better or worse, loss of our scientific expertise to foreign governments is one of the prices we pay for the freedom of research and publication guaranteed by the First Amendment.

expose the individual to a surveillance that would invade his most sensitive communications. Given the eagerness of some administrations to know what is going on in law firms, commodity lobbies, and other political and business groups with foreign connections and clients, I do not think this power should be given to the Executive branch, even if the minimization procedures were more stringent than they were in this bill. Indeed, I am surprised that multi-national corporations are not up in arms over this bill. Section 2521 (b)(B)(i) is a "sleeper provision" which, if read in conjunction with the Export Administration Act's prohibitions on the export of certain materials, information, and technology to "Communist-dominated" countries could give the CIA and the White House a substantial economic and political weapon against companies and industries they wish to manipulate or punish.

Nor need Congress permit easy surveillance of law firms, advertising agencies, multi-national corporations, and other U.S. representatives of foreign firms in order to punish deliberate spies like Heine. An amendment to the espionage laws could make probable cause warrants possible by declaring it a crime to transmit certain kinds of defense-related information to a foreign power without special clearance where the individual knows that the information has been requested by, or on behalf of, a foreign intelligence agency or network, or a foreign defense establishment.

Drafting such a provision would take time, but I cannot imagine that the temporary lack of authority to wiretap researchers in the New York Public Library would cripple our counterintelligence efforts. One way to find out would be to ask the FBI how many electronic surveillances of the *Heine* variety it is conducting now. My guess is that there are none.

Hypothetical No. 2.—The second hypothetical advanced in support of the non-criminal standard for pseudo-warrants is the case of a person who slinks about like a spy:

> Pursuant to the physical surveillance of a known foreign intelligence officer, B is seen to clear dead drops filled by that officer. On the second Tuesday of every month B drives by the officer's residence, after engaging in driving maneuvers intended to shake any surveillance. Within 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 employee of the opposite sex specializing in matters dealing with the country of the intelligence agent.

The Justice Department assumes, and the ACLU agrees, that the government would have probable cause under the Espionage Acts to wiretap B and the intelligence office.[9] But the Justice Department wants to tap the phone and bug the bedroom of the State Department lover and for that, it knows, it lacks probable cause.

Again, my answer is "tough." The Fourth Amendment exists to protect the privacy of innocent lovers, even at some cost to the efficiency of counterintelligence investigations. Cases will vary, but wiretapping and bugging are not the only ways to determine whether presumptively innocent lovers are really spies.[10]

Hypothetical No. 3.—The Justice Department's third hypothetical postulates that

> 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 information, but the information carried, which is not available to the public, when put together, can give valuable information concerning components which are used in United States weapons systems.

Super-broad spy powers are not needed to capture these spies; Congress can simply amend the Omnibus Crime Control and Safe Streets Act of 1968 to

---

[9] This, I take it, is a retreat from the Department's earlier position (not published, to my knowledge) that probable cause would not exist unless the FBI could prove that classified information was being transmitted through the dead drop.

[10] In this case one way would be to arrange a temporary reassignment for the lover to see if the loading of the dead drop stops. Another would be to inspect the dead drop, if possible, to see whether documents from the lover's office are being transmitted. A third would be to plant a "test document" with the lover and see if it comes out at the other end of the pipeline, assuming that there is a way of finding that out. A fourth would be temporarily to cut off the lover's access to classified information (in a way that does not harm his or her career) and see if the love affair is terminated.

make it is a crime to intercept digital communications transmitted within interstate communications grids. This should have been done years ago, when Professor Arthur R. Miller first proposed it, simply to protect the confidentiality and privacy of those communications. Miller, *Assault on Privacy* 162–163 (1971).

Hypothetical No. 4.—Hypothetical No. 4 is the Perennial Pimp Problem:

> D, a headwaiter in a fashionable Washington, D. C. resturant, acts as a bookmaker and procurer for several well-known and highly placed customers. A [reliable] 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.

As I read the hypothetical, it attempts to postulate a situation in which the information sought is simply "embarrassing and personally damaging" and therefore does not trigger application of the federal extortion statute, which requires information that the person to be blackmailed has violated the law. Furthermore, the extortion law might not come into play because there is no link to interstate commerce.

The problem posed by this hypothetical goes far beyond mere intelligence collection; blackmail and bribery threaten the very integrity of the democratic process. But again, the most sensible solution would be to amend the criminal law to make it a crime to blackmail public officials, just as it is now a crime to bribe them (18 U.S.C. Section 201) and to add blackmail of public officials to the list of crimes (including bribery of public officials) for which wiretapping is a permissible investigatory technique. 18 U.S.C. Section 2516. Section 1357 of the proposed revision of the Federal Criminal Code would seem to lay the criminal predicate by making it a crime to "tamper with a public servant."

Hypothetical No. 5.—The Justice Department's fifth case postulates a burglar seeking stray scraps of classified information lying around the homes or apartments of government officials holding sensitive positions:

> A [reliable] 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 information concerning United States positions at the U.N.

Here I agree with the ACLU; the hypothetical is frivolous. Physical surveillance rather than wiretapping is the more likely way in which a burglar will be caught in the act. But where, as here, there is probable cause to believe that the burglar is engaged in a conspiracy to commit espionage, a criminal warrant already is available. 18 U.S.C. Section 2516(1)(a).

Hypothetical No. 6.—The final hypothetical argues for electronic surveillance in the very earliest stages of a possible espionage operation.

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

The point of this hypothetical is far from clear. If the FBI wants to tap the phones or bug the rooms of refugee organizations, it should be denied the power for obvious First and Fourth Amendment reasons. If it wants to tap F, it may already have authority under the 1968 Act to do so, on the theory that a conspiracy to infiltrate the CIA and the FBI is presumptively a conspiracy either to commit espionage or to obstruct justice. 18 U.S.C. Section 2516(1)(a) and (c) respectively.

Third country spying.—There is one other hypothetical not on the official list of six that has been advanced from time to time to illustrate a need for non-criminal warrants. It involved "third country spying"—spying in the United States not against the United States, but against a third country. Such spying, Justice Department officials have argued, is not espionage against the United States.

Actually, that is not entirely true. Under 18 U.S.C. Sec. 781, it is an offense for anyone to "knowingly and willfully make any sketch, photograph . . . map,

model . . . or any other representation of any vessel, aircraft, equipment or other property relating to the national defense . . . awaiting delivery to . . . the government of any country whose defense the President deems vital to the defense of the United States. . . ." It would be interesting to know why the Justice Department regards this law as inadequate to the FBI's investigative needs. Perhaps it is because laws against spying are no help in establishing federal jurisdiction to investigate foreign agents from rival countries who, while on American soil, violate state law in their attempts to do each other in.

Whatever the reason, criminal jurisdiction could be established by adding failure to register as a foreign agent to the list of crimes for which probable cause warrants now may issue under title III of the Omnibus Crime Control Act. This solution is advocated in the House version of this bill, H.R. 3632, sponsored by Representative Kastenmeier. However, if the registration acts are used as a predicate for probable cause warrants, the Congress should make it clear that it adopts the narrow reading of them employed by Judge Hand in the *Heine* decision. In that case, Heine's other conviction—for failure to register as a Nazi agent—was upheld because the court could find, within the legislative history, an intention to use the act mainly against spies. 151 F. 2d at 816–817. Appropriate language in the Committee's report on S. 1566 could make it clear that the surveillance authority granted by reference to the registration acts does not encompass all persons who might be nominal "foreign agents," but only the officers, employees and paid informants of any foreign intelligence or network.[11]

If this were done, the government would not need the broad powers it seeks in order to deal with the hypotheticals it has raised. In each instance, warrants would be available on a showing of probable cause.

Of course, the Justice Department would have this Committee believe that the probable cause standard is too high and that the federal judiciary might prove unsympathetic to national security warrant applications. Given the extraordinary deference which federal judges have paid to vague claims of national security over the years, the assertion seems preposterous.

Moreover, it is common knowledge that warrants for electronic surveillance are given out like candy. Between January 1969 and December 1975 the federal government sought 1,066 warrants under title III and was turned down only once. "Annual Reports on Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications," Administrative Office of the United States Courts, Washington, D.C. When the Justice Department is getting 99.9 percent of all the warrants it requests, it takes chutzpa to claim that the nation's security will be threatened unless the probable cause standard is not watered down further.[12]

CASE OR CONTROVERSY

Quite apart from the Fourth Amendment, there is reason to doubt whether federal courts would have jurisdiction to issue the non-criminal warrants authorized by this bill. Article III, Section 2, of the Constitution provides that the judicial power of the United States shall extend only to "cases" and "controversies." Traditional search warrants, as an integral element in a developing "case," would seem to fall within the judicial power of the United States, and so the courts have always assumed. But the information sought pursuant to this bill's warrants would have nothing to do with criminal "cases." Accordingly, by what authority may a court issue them? [13]

---

[11] Similar registration requirements could create federal criminal jurisdiction to investigate foreign terrorists or sabotage activity against private persons and property, or against officials and property of state or local governments.

[12] This is the same Justice Department which, in 1975, sought and obtained two warrants from a federal district judge under title III even though, as it told the court, it lacked probable cause to believe that any of the crimes listed in that act had been, or were about to be committed. Justice Department memorandum cited in the Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, U.S. Senate, 94th Cong., 2d Sess. (1976), Book III 292–93, n. 71.

[13] For discussions of this issue see Robert H. Jackson, *The Supreme Court in the American System of Government* at 12 (1955); Telford Taylor, *Two Studies in Constitutional Interpretation* at 85–88 (1969); and the testimony of John P. Walsh in *Wiretapping*, Hearings Before Subcommittee No. 57, Committee on the Judiciary, U.S. House of Representatives, 84th Cong., 1st Sess. (1955), at 239; Murray Gordon, *id.* at 234–39; Charles A. Reich in *Wiretapping and Eavesdropping Legislation*, Hearings Before the Subcommittee on Constitutional Rights, Committee on the Judiciary, U.S. Senate, 87th Cong., 1st Sess. (1961), at 183–84; and Herman Schwartz, *id.* at 411.

THE SEVEN HANDPICKED JUDGES

Not satisfied with a 99.9 percent acceptance rate on probable cause warrants, the Justice Department has insisted on limiting the number of judges who can issue psuedo-warrants to seven, and demands that each be chosen by the Chief Justice.

As Professor Louis Henkin of Columbia Law School noted in his testimony last year before a House Judiciary subcommittee, "the bill contemplates . . . handpicked judges." It loads "the dice very heavily in favor of the search and against the individual right." Foreign Intelligence Surveillance Act. Hearings Before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice, U.S. House of Representatives, 94th Cong., 2d Sess. (1976) at 74.

All of the incentives run in favor of granting applications. A judge who refuses must pay the penalty of writing an opinion and must run the risk of being overruled. On the other hand, granting applications requires no work and involves no risk. Section 2523.

The bill goes further and permits judge-shopping in two directions. First, if one of the handpicked judges develops a reputation for skepticism, the government can avoid him forever. Indeed, there is nothing in the bill to prevent the government from taking all of its applications to the most gullible or pro-government judge on the bench.

Second, if for some reason the government choses the "wrong" district court judge, it is entitled to two new hearings euphemistically called "appeals." Of course these are not appeals in the traditional sense, since the government will rarely be questioning a ruling of law. Rather, they will be de novo hearings on the factual questions: is the target a "foreign power" or "agent of a foreign power?" Accordingly, the higher court will not employ the usual presumption that the trial judge's assessment of the facts was correct.

In an ordinary case of treason, espionage, or sabotage, the government has no right to appeal the denial of a warrant; the decision of the trial judge is final. Why would the government get two appeals on matters of lesser importance? Moreover, the government gets to argue both "appeals" unopposed. The bill does not even permit the district court judge to defend his ruling at these secret proceedings.

In my opinion, the appeals procedure should be scrapped. There is no reason why the government should have three de novo hearings on the same intelligence warrant, when in all criminal cases it is entitled only to one. Given the few appeals that are likely (about one every eight years), the review structure is totally unnecessary.[14] In light of all the advantages this bill now gives the intelligence agencies, for them also to insist on appeals smacks of greed.

Furthermore, there is no reason why the FBI should not take its chances with any judge now sitting on the federal bench. To imply that judges as a class are more prone to leak than, say Justice Department employees, is an insult to the judiciary and an affront to common sense.[15] Certainly the storage of documents poses no problem that can't be solved with a little ingenuity, as the Court pointed out in *Keith*. 407 U.S. at 321.

Nor is there any reason to believe that every district court would have to be equipped with the latest GSA-approved security containers. If the government's figures from past years are accurate, there should be about a hundred and sixty warrant applications each year. If I had to make a guess, 80 or 90 will be sought annually in Washington, 30 or 40 in New York, and the rest in three or four other major cities. Thus, as a practical matter, this means the installation of security containers in perhaps a half-dozen courthouses for the very occasional use of no more than fifteen judges.

---

[14] Under the more stringent probable cause standards, denials would occur in approximately .0009 cases annually. Assuming that there are about 159 applications each year (the average number of taps and bugs used annually for national security purposes from 1965 to 1976), an appeal might occur once every ten years. Yearly averages from Church Committee hearings, Vol. 5 at 69–70.

[15] It is instructive, I think, that the Justice Department has not cited a single breach of judicial security in seven years experience under title III. Attorney General Bell put it best in testimony last June before the McClellan subcommittee: "The most leakproof branch of the Government is the Judiciary." *Foreign Intelligence Act of 1977*. Hearings Before the Subcommittee on Criminal Laws and Procedures. Committee on the Judiciary. U.S. Senate, 95th Cong., 1st Sess. (1977), p. 27. Moreover, if the government is so afraid of judges leaking information from warrant applications, why is it willing to give *any* federal judge in America the records of an entire sensitive surveillance, possibly involving discussions of the nation's most closely held secrets, for *in camera* inspection at time of trial?

However, if the Committee believes that federal judges are so untrustworthy a class that a select few must be chosen, then the number should be raised to twenty-two—one principal judge and one alternate for each judicial circuit—and the selection should be placed where it normally resides, with the chief judge of each circuit who has the power to designate judges within his circuit for special review. Provision could be made for the appointment of additional judges in the rare event that the principal judge is in danger of being drowned by a flood of applications. Giving the assignment task to a busy Chief Justice, who cannot possibly know all of the judges from whom the selection should take place, seems an unnecessary burden, as well as a possible affront to the integrity of the lower courts. To some, it may even suggest an unworthy scheme to assure that only pro-government jurists will be chosen in the first round.

Assigning judges by circuit also would make it possible to eliminate horizontal judge-shopping by limiting each judge's mandate to his circuit only. In turn, that would assure that no one judge is "burdened" with too many applications. A fixed term, say of five years, ought to be set so that the appointing authority cannot assert a power of removal.

In addition, there is no reason why the government should be free to plead for its warrant unopposed. The target of the surveillance may not be represented, but that should not bar Congress from authorizing the judges to seek assistance from a properly cleared *amici curiae*. Given the few applications that are likely to be handled each year, and Congress' obvious interest in the matter, it might make sense to allow the judges to call upon the staff counsel of the intelligence committees.[18] So long as the counsel function as friends of the court, no separation of powers problem should arise.

HOW COMPELLING IS THE NEED?

The Justice Department and its clients continue to insist that the need for counterintelligence taps and bugs is compelling. The need is so great, they argue, that the traditional Fourth Amendment requirement of probable cause should be swept aside.

While the need for taps and bugs may be compelling in the context of a given espionage, sabotage, or treason case, the overall significance of the technique is questionable. Former Attorney General Ramsey Clark has testified that if all national security intelligence taps were turned off, the adverse impact on national security would be "absolutely zero." *Warrantless Surveillance*. Hearings Before the Administrative Practice and Procedure Subcommittee, Committee on the Judiciary, U.S. Senate, 92d Cong., 2d Sess. (1972), p. 53. Attorney General Levi testified that he had found no reason to use the power against Americans (Church Committee Hearings, Vol. 5, p. 90), and FBI Director Kelley testified last June that no Americans were then targets of national security electronic surveillance. *Foreign Intelligence Surveillance Act of 1977*. Hearings Before the Subcommittee on Criminal Laws and Procedures, Committee on the Judiciary, U.S. Senate, 95th Cong., 1st Sess. (1977), p. 24.

Another skeptic is William C. Sullivan, former assistant to the Director of the FBI and head of its intelligence section. In a paper prepared in 1974, Sullivan urged that "Consideration be given to (ordering) that no telephone surveillance or microphones be used by any federal agency during the next three years. At the same time a vehicle should be set up to study . . . the effects of this ban to determine if the criminal and security-intelligence investigations suffered . . . or not." *Privacy and a Free Society* at 99 (1974).

William Sullivan was not one to play fast and loose with the national security. If he thought so little of electronic surveillance as to propose banning it entirely for three years, then the proponents of this bill clearly have a heavy burden of persuasion to carry.

Just to be sure, this Committee might ask the FBI to review all of its espionage prosecutions and spy deportations since World War II and report any instances in which electronic surveillance provided significant evidence or crucial leads. If my suspicions are correct, that report will be very short.

---

[18] Dean Louis Pollak of the University of Pennsylvania Law School has proposed that opposition counsel be drawn from the Department of Justice. *Foreign Intelligence Surveillance Act of 1976*, Hearings Before the Subcommittee on Criminal Laws and Procedures, Committee on the Judiciary, U.S. Senate, 94th Cong., 2d Sess. (1976) at 63.

POSITIVE INTELLIGENCE

The primary purpose of this bill is not to enhance counterintelligence operations, but to legitimize the much broader, less focused, and less controllable positive intelligence operations of the FBI, the CIA, and the National Security Agency. The hypotheticals about non-criminal spying are red herrings; the main objective of this bill is to obtain Congressional blessing for taps and bugs directed at foreign embassies and consulates, the homes of diplomats, military attaches, and embassy legal officers, the hotel rooms and offices of foreign trade delegations, the boardrooms of selected corporations dealing in strategic commodities like wheat and oil, and the telephones of Washington law firms with foreign governments and corporations as their clients.

If there is a counterintelligence purpose to this bill that cannot be accomplished through the investigation of crimes, it is to gather information to blackmail foreigners into spying for the United States or to facilitate "preventive action" operations against the so-called "legal spies" attached to foreign embassies.

There has been virtually no public inquiry into these purposes of the bill. In part, that silence is due to concerns for secrecy and fear of international embarrassment; no one wants to force our government to admit officially what every foreign government knows unofficially. For the most part, however, I suspect that the intelligence agencies deliberately discourage inquiries into their diplomatic surveillance operations for fear of dispelling a number of myths which aid the annual search for appropriations. They want Congress to go on believing that such monitoring is cost efficient. They do not want to admit that the installation of embassy bugs often requires the commission of burglaries with the "flap potential" of the U–2 incident, and, most of all, they do not want Washington politicians to realize that it is their conversations with foreigners that are of greatest interest to the embassy tappers.

EMBASSY SURVEILLANCE

The primary function of wiretaps on the domestic telephone lines into foreign embassies is not to uncover spies. The military attaches, legal officers, and political officers who conduct that function know better than to communicate with their sources over these lines, and they would shun those telephones even if Congress banned embassy tapping altogether. The chief function of embassy tapping is to know who is talking to foreigners about what.

For example, in the early 1960's, Attorney General Kennedy authorized the FBI to use electronic surveillance against certain foreign targets in Washington, D.C., in order to learn more about the attempts of a foreign government to influence Congressional action on sugar imports. From this surveillance, the Attorney General received significant information not only about possible foreign influence on the Congress, but about the views of key members of the House Agriculture Committee on the Administration's proposed sugar quota.

In 1966, President Johnson directed the FBI to report to him on all contacts between Senators, Congressmen, and prominent citizens and the representatives of certain foreign countries. From May 1966 until January 1969, Johnson received biweekly reports on members of Congress and their staffs.

Johnson also ordered the FBI to put the South Vietnamese embassy under electronic surveillance because he suspected the Mrs. Anna Chennault, a prominent Republican, would attempt to persuade South Vietnamese officials to boycott the Paris peace talks.

In addition to these political uses of embassy wiretaps, reported by the Church Committee (Final Report, Book III at 313–315, 340), the FBI also kept separate files on the embassy calls of American journalists. Morton H. Halperin, "The Administration's Wiretap Reform Bill—S. 1566," *First Principles*, June 1977, p. 6.

MINIMIZATION

S. 1566 would not effectively end these abuses. Where the so-called "foreign power" warrants are concerned, the judge's role is very limited. He can decide whether there is probable cause to believe that the target is a foreign power and that the facilities or place to be monitored are being used by a foreign power, but beyond that all he can do is decide whether the government's promise to minimize the invasion of privacy sounds plausible. Section 2525(a)(3) and (4). Like the infamous writs of assistance that so angered colonial Boston, these so-

called warrants are not returnable. Unless the government returns to the original judge for a renewal of the authorization, there is no way in which a judge can scrutinize the "take," check FBI files, or otherwise determine that the minimization promises were kept.

Failure to make these warrants returnable raises jurisdictional problems. The Supreme Court's decisions on what constitutes a "case" or "controversy" are far from lucid, but a procedure that makes subsequent adversary challenge impossible would seem to violate Article III, Section 2, of the Constitution.

The minimization procedures do nothing to prevent the continued storage of tapes and logs of conversations involving legislators and journalists or other Americans, provided that those conversations somehow "relate to . . . the security of the nation (or) the conduct of foreign affairs." Section 2521(b)(8). "Marginally related to" would seem to suffice, for the bill does not insist that the information be "necessary" or "essential" to either purpose. This loophole alone transforms the minimization procedures of the bill into an elaborate hoax.

Nothing in the bill would guarantee that appropriate committees of Congress would audit the files, logs, and tapes on a systematic basis. Section 2527 provides for statistical reports only. Given the excellent record of this committee and its predecessor in safeguarding the privacy of individuals, there is no reason why auditing procedures should not be arranged. Should Congress return to its old ways, there will be time enough for the executive branch to deny access again.

The controls on dissemination and use are likewise weak. Nothing in the bill requires the judge to see to it that the government is complying with the rules governing dissemination and use. Because the government is free to use and disclose information for the undefined purpose of providing for the "security of the nation," it is free to engage in "preventive action" abuses of the sort the Church Committee so recently disclosed.

Notice of the search has traditionally been regarded as an integral element of the judicial warrant procedure. However, S. 1566 would deny defendants the right to examine the logs and tapes that may be used against them, unless invited to do so by a puzzled judge. Section 2526(c). Whenever the government fears for its security (and when doesn't it?), the judge must examine the documents *in camera* and make a secret determination as to whether the defendant's rights were violated. If the judge decides that the surveillance was lawful, information based on it can be introduced without the defendant knowing whence it came. Unlike the government, which can pick its judge and appeal the denial of a warrant, the defendant has no choice of judge and no knowledge on which to challenge the judge's decision on appeal. Justice may be blind, but whoever drafted section 2526 was not.

In short, the "foreign power" warrant provisions are a sham. They do nothing to restrain the Executive branch and they make a mockery of the courts.

THE LEGAL BASIS OF "FOREIGN POWER" SURVEILLANCE

The legal basis of the "foreign power" warrant provisions is far from clear.

Under international law, the United States has a duty 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). Article 11 of the Vienna Convention on Diplomatic Relations, 23 U.S. 3237–38, provides:

1. The premises of the mission shall be inviolable. The agents of the receiving States may not enter them, except with the consent of the head of the mission.

2. The receiving State is under a special duty to take all steps to protect the premises of the mission against any intrusion . . .

3. The premises of the mission, their furnishings and other property thereon and the means of transport of the mission shall be immune from search, ...

In addition, Article 30 extends the same protection to the "private" residence of a diplomatic agent." 23 U.S. at 3240.

In 1976, Attorney General Levi assured a House Judiciary Subcommittee that this bill (in its earlier incarnation) was not inconsistent with our obligations under international law. *Cong. Rec.*, June 3, 1977 at H5423.. To support his argument, Levi referred to a legal memorandum prepared by his Office of Legal Counsel, which he permitted members of the subcommittee to read, but which he refused to make public. One can only guess that the Department has chosen to interpret both the Geneva Convention and customary international law to bar

physical "invasions," unauthorized entries, and physical searches for tangible items, but to permit the use of telephone company wiretaps and eavesdropping by parabolic microphones beamed from outside. It is also possible that the Department would not regard a bug carried by, or planted by, an inside informant or "unofficial" person as a violation of international law. And, given the general practice of nations, it would probably be inappropriate to read the Geneva Convention more broadly.

However, as I read S. 1566, it contemplates microphone surveillance of embassies which would require surreptitious entries in this country. If not, then the Nixon administration against Chilean diplomats in this country. If not, then the bill should say so in no uncertain terms. If so, then perhaps Congress may wish to reconsider the wisdom and propriety of directing our courts to rubber stamp executive decisions abrogating international law.

If Congress rejects the "clean slate" theory of this bill and agrees that the Fourth Amendment protects all persons on American soil, then it also should reconsider the constitutional basis of "foreign power" taps and bugs. Attorney General Levi's solution was to make all non-resident aliens Fourth Amendment outlaws. My own preference is for something less drastic.

The most sensible solution may be to treat electronic surveillance of embassies and consulates (and perhaps the private residences of persons bearing diplomatic passports or credentials) as a new category of "routine" searches, like customs inspections, for which *no warrant* is necessary. If S. 1566 made it clear that certain facilities and telephones of foreign powers located in the United States are not immune from national security or foreign intelligence electronic surveillance at the direction of the President, it would effectively put people on constructive notice not to harbor any "expectations of privacy" when telephoning or visiting those facilities.

The bill could identify the "places to be searched" as belonging to, or principally occupied by, persons enjoying diplomatic immunity. This would help obviate the Fourth Amendment's concern with warrantless searches for incriminating evidence, and would permit use of the concept of "assumption of the risk" to rebut diplomatic claims to Fourth Amendment warrant protection.

Elimination of the "foreign power" warrants would hardly be regressive; they are only rubber stamps now. Elimination would save the courts from embarrassment and the public from a deception. At the same time, the elimination of "warrants" for this kind of surveillance would not prevent Congress from imposing substantial use restrictions and providing for auditing and minimization. Whether these restrictions could be administered by the courts is doubtful; jurisdiction of the federal courts requires the existence of a case or controversy and an application for an *ex parte* order that does not fit the traditional definition of a warrant might not fulfill that requirement. Administrative supervision with legislative auditing, however, could suffice. Precedent for legislation regulating warrantless searches under the Amendment's first clause can be found in 19 U.S.C. Sec. 482, as recently interpreted by the Supreme Court in *United States* v. *Ramsey*, 45 U.S.L.W. 4577 (June 6, 1977).

If this approach makes embassy taps and bugs constitutional, it does nothing to legitimize the surveillance of visiting trade delegations, journalists, or others whom the government would like to tap and bug, mainly for economic and political intelligence. For reasons which I shall now develop, I do not believe electronic surveillance of non-resident aliens is permissible under the Fourth Amendment without full warrant clause protection.

NONRESIDENT ALIENS AND THE FOURTH AMENDMENT

When this bill was first conceived, the Justice Department took the position that nonresident aliens are not "people" within the meaning of the Fourth Amendment. Reviving a theory used by A. Mitchell Palmer to justify his infamous "Red Raids," Attorney General Levi told the Church Committee that the only "people" protected by the Constitution against unreasonable searches and seizures are "We, the people" who "ordain and establish this Constitution." Church Committee Hearings, Vol. 5 at 74.

It was a shameful theory, internally illogical and at variance with fifty years of judicial doctrine. Quite predictably, the Carter administration has abandoned it for the seemingly more reasonable assertion that "the Fourth Amendment protects aliens in the United States as well as United States citizens," but that the standards for issuing warrants can differ. *Foreign Intelligence Surveillance*

Act. Hearings Before the Subcommittee on Criminal Laws and Procedures, Committee on the Judiciary, U.S. Senate, 95th Cong., 1st Sess. (1977), pp. 16, 32. In other words, all persons are equal under the Fourth Amendment, only some are more equal than others. S. 1566 embodies this Orwellian spirit:

Where the privacy of "U.S. persons" is at stake, the judge can lift the veil and look behind the government's certificate of need to make certain that it is not "clearly erroneous." But if the privacy of a nonresident alien hangs in the balance, the judge may not look. Section 2525 (a) (5).

The minimization procedures are designed to protect U.S. persons only. The government can acquire, retain, and disseminate all the information it pleases on nonresident aliens, free from any judicial restraint whatever. Sections 2521 (b) (8) and 2526. Among other things, this lack of protection would open nonresident aliens to a variety of "dirty tricks," including blackmail to persuade them to spy for the United States and disclosure of their whereabouts to a foreign intelligence agency seeking to kill them.

Notice of a wrongful emergency use of electronic surveillance may be served on a U.S. person, but not on a nonresident alien. Section 2527(d).

A statutory cause of action against violators of this act is granted to U.S. persons, but not to nonresident aliens who, like many people who live in socialist countries, are only nominal "officer(s) or employee(s) of a foreign power." Section 4(j) on p. 29.

It is common knowledge that Congress has broad authority to regulate the conditions under which aliens can enter this country, remain here, apply for citizenship, and enjoy health, education, and welfare benefits. But this bill has nothing to do with the exercise of those powers. What it asserts is that there are two Fourth Amendments: one for citizens (and, by legislative suffrance, for resident aliens), the other for nonresident aliens. However, the Fourth Amendment draws no distinctions among "people." It does not condition the right to be free from unreasonable searches and seizures on acceptance of U.S. nationality; it extends the right indiscriminately and comprehensively to all "people." The same policy is evident in all the guarantees of the Bill of Rights.

The logic of this constitutional policy should be obvious. Creation of a class of First, Fourth, Fifth, or Sixth Amendment "outlaws" would affect us all, just as it affected those loyal Americans who, because of foreign-sounding names or alien relatives, were swept up in the anti-German persecutions of World War I, the Red Raids of 1919 and 1920, and the Japanese internment of World War II.

Of course, both federal and state law has long discriminated against aliens in matters of employment, property holding, licenses to practice professions, and entitlement to welfare benefits. Cushman, *Cases on Constitutional Law*, 4th ed. at 652–54 (1975). In recent years, the Supreme Court has moved vigorously against state discrimination, subjecting it to the strictest scrutiny under a "suspect classification" test. E.g. *Graham* v. *Richardson*, 403 U.S. 365 (1971) and *Sugarman* v. *Dougall*, 413 U.S. 634 (1973). Deference to federal classifications continues, but at a somewhat higher level of scrutiny than before. *Hampton* v. *Mow Sun Wong*, 426 U.S. 88 (1976), but see *Mathews* v. *Diaz*, 426 U.S. 67 (1976).

Where Fourth Amendment rights are concerned, the courts have rejected a double standard for aliens. As early as 1920, the Second Circuit Court of Appeals, in an opinion by Judge Hand, ruled that the Fourth Amendment's full protection extends to foreign nationals. *In re Weinstein*, 271 F. 673 *aff'g* 271 F. 5. Three years later, the Supreme Court held that an alien could invoke the exclusionary evidence rule in a deportation proceeding. *United States ex rel. Bilokumsky* v. *Tod*, 263 U.S. 149 (1923). And, in 1960, all nine justices of the Court agreed that even a Soviet espionage agent who entered the United States illegally was entitled to full Fourth Amendment protection. *Abel* v. *United States*, 362 U.S. 217 (1960).

It may be argued that the majority in *Abel* actually made an exception to the principle of Fourth Amendment equality by upholding the admissibility of evidence obtained in a planned search by Immigration officials acting without a judicial warrant, but with an administrative warrant which Congress authorized in deportation cases. The Court split 5–4 on this issue. However, with the demise of the *Rabinowitz* theory of an independent reasonableness clause, and the passing of arrest warrants, *United States* v. *Watson*, 423 U.S. 411 (1976), that dispute is moot. What remains of *Abel* today is the unanimous principle that the Fourth Amendment applies to all "people" equally. As the Seventh Circuit Court of Appeals ruled last year, even the plenary power of Congress to deport aliens "cannot be interpreted so broadly as to limit the Fourth Amend-

ment rights of those present in the United States." *Illinois Migrant Council* v. *Pilliod*, 540 F. 2d 1062 (7th Cir. 1976).

Such, at least is the state of Supreme Court doctrine. Given the deference which the Court still shows for both Congressional regulation of aliens and claims of national security, it is possible that the current court might depart from precedent and uphold the anti-alien provisions of S. 1566. Much probably would depend on the context in which the first case arose. If the defendant is convicted of espionage, the Court can be expected to lean over backwards to keep him in jail. If he is a visiting foreign student, caught up in a dragnet surveillance, the anti-alien provisions might be struck down.

However, what the Supreme Court may or may not do with this bill is essentially beside the point. Congress must decide the constitutionality of the bill's anti-alien provisions in the first instance. In so doing, it should be aware that neither case law nor the concept of equal protection evident in the wording of the entire Bill of Rights supports the government's theory of two Fourth Amendments. To enact the anti-alien provisions is to set a statutory precedent for still further discrimination against aliens at a time when both Congress and the courts have been moving to end that discrimination.

Were the pseudo-warrants authorized by this bill limited to the surveillance of embassies and consulates, it would be difficult to raise a Fourth Amendment, equal protection objection. Or, if the surveillance were limited to nonresident aliens serving as officers, employees, or paid informants of a foreign intelligence agency, military establishment, or diplomatic corps, an exemption from all or part of the Fourth Amendment might be reasonable. However, this bill sweeps far beyond, raising serious questions of constitutional overbreadth. Section 2521's definition of "officer(s) or employee(s) of a foreign power" would permit easy tapping and bugging of subway conductors from Paris, doctors from Great Britain, and professors from West Germany. Such persons could well be your relatives or mine, here on a holiday. I see no reason why they should be treated differently from us. But if this bill passes in its current form, they most certainly will be, and visiting the United States could become as unpleasant for foreigners as going to the Soviet Union or South Korea now is for Americans.

RIGHTS OF U.S. PERSONS OVERSEAS

To the extent that Congressional supporters of this bill have persuaded the President to admit that his power to tap and bug for intelligence purposes is limitable by legislation, they have achieved an historic advance. Unfortunately, the bill seems to substitute legislative power for executive power without acknowledging that both Congress and the President are bound to legislate within the limits of the Fourth Amendment.

Nowhere is this "clean slate" theory more evident than in the provision defining the kinds of "electronic surveillance" regulated by this bill. As I read Section 2521(b)(6), it assures that the bill will do nothing whatever to curb:

Wiretapping of U.S. persons overseas by the CIA and the military;

Bugging of U.S. persons abroad by the CIA and the military;

Interception of the long distance telephone calls and cables of U.S. persons abroad to other persons abroad by the National Security Agency through computerized searches of microwave transmissions;

Monitoring, by microwave interception and cable-tapping, of communications from U.S. persons located abroad to nonresident aliens in the United States;

Monitoring, by the same means, of telephone calls and cables from foreigners abroad to U.S. persons in the United States, provided that the contents of the message are not acquired by "intentionally targeting that U.S. person."

By failing to plug these holes, Congress gives the impression that it believes that Americans lose their constitutional right against unreasonable searches and seizures the moment they leave our shores. Moreover, it invites future Presidents to assume that they have an "inherent power" to violate the privacy of hundreds of thousands of Americans who live and work abroad.

Most Americans are not aware of the extent to which their government has spied on its citizens abroad. A typical example occurred in West Berlin in 1972 and 1973, where Army intelligence infiltrated an affiliate of the American Democratic Party, infiltrated a German church mission in order to spy on American ministers, persuaded German authorities to wiretap American attorneys and journalists, and persuaded private employers to deny several Americans

their jobs. The monitoring was carried out, the Army later claimed, to protect national security and foreign relations, although it admitted that it did not have any reason to believe that the Americans were agents of a foreign power. Information collected included the names of persons signing a petition calling for the impeachment of President Nixon and confidential lawyer-client communications. Asked to explain where it got the power to spy on American political activity overseas, the Army cited its Status of Forces Agreement with West Germany. *Berlin Democratic Club* v. *Rumsfeld*, 410 F. Supp. 144 (1976) and *Military Surveillance*, Hearings Before the Subcommittee on Constitutional Rights, Committee on the Judiciary, U.S. Senate, 93rd Cong., 2d Sess. (1974) at 106. See also Pyle, "Spies Without Masters: The Army Still Watches Civilian Politics," 1 *Civ. Lib. Rev.* 38 (1974).

This was not the first instance in which the military claimed that the Bill of Rights could be suspended by a mere exercise of inherent executive power. In 1950, the First Circuit Court of Appeals rejected a claim that the Fourth Amendment did not protect the premises of an American citizen in Vienna from a U.S. military search. *Best* v. *United States*, 184 F. 2d 131 (1st Cir. 1950), *cert. denied*, 340 U.S. 939 (1951). The Court of Claims later ruled that the Fifth Amendment's just compensation clause applies to the seizure of the overseas property belonging to Americans and cannot be nullified by executive agreements with foreign governments. *Turney* v. *United States*, 115 F. Supp. 457, 464 (1953); *Seery* v. *United States*, 127 F. Supp. 601 (1955). See also Sutherland, "The Flag, The Constitution, and International Agreements," Comment, 68 Harv. L. Rev. 1374 (1955). In 1957, the Supreme Court declared that not even the combined foreign affairs powers of the President and Congress were sufficient to abrogate the Constitutional rights of Americans overseas. 354 U.S. 1, 16 (1957).

In light of these cases, it seems to me that Congress is under a constitutional obligation to bring all forms of electronic surveillance by the United States against U.S. persons located abroad under a Fourth Amendment warrant system.[17]

NSA MICROWAVE INTERCEPTS AND THE FOURTH AMENDMENT

The fact that the Fourth Amendment rules out deliberate warrantless electronic surveillance of U.S. persons by their government anywhere poses special problems for the National Security Agency which routinely searches microwave radio transmissions and international cable traffic for sensitive information. Testimony of Gen. Allen, Church Committee Hearings, Vol. 5, 5–55.

S. 1566 would require the government to obtain pseudo-warrants before intercepting any domestic microwave transmissions. Pseudo-warrants also would have to be obtained before targeting U.S. persons located in the United States who receive communications from abroad. However, the bill would leave NSA completely free to eavesdrop on U.S. persons located abroad communicating with others located abroad, or with nonresident aliens in the United States. And it would permit the use of communications of U.S. persons "incidentally" intercepted by watchlisting their foreign associates. Section 2521 (b)(6). These loopholes imply the existence of "inherent" executive powers inconsistent with Fourth Amendment principles.

It is not difficult to understand why the Justice Department is reluctant to acknowledge the constitutional rights of Americans *vis-a-vis* NSA overseas. To do so would be to admit that the Agency may not collect economic and political intelligence from the communications of overseas Americans. Monitoring the communications of drug traffickers, terrorists, and spies would still be possible, but listening to Mobil Oil executives in Africa, midwestern grain dealers in India, and Pepsi-Cola representatives in the Soviet Union would be impermissible.

I wonder if the general counsels of major U.S. corporations engaged in international trade realize the extent to which this bill would legitimize federal surveillance of their most confidential business transactions.

---

[17] The absence of a magistrate or judge located abroad has been held to be an insufficient reason for not doing so. *Berlin Democratic Club* v. *Rumsfeld*, 410 F. Supp. at 160. See also *United States* v. *Robinson*, 533 F. 2d 578 (D.C. Cir. 1976); approving the communication of warrant requests by telephone, provided that they are "based on sworn oral testimony . . . with procedures for recording, transcribing and certifying the statement."

Finally, it seems to me that this bill's priorities and values come through most clearly in Section 2525 (b)(2)(B) and (C) which would enable the Justice Department to get orders directing landlords, custodians, and other persons to help install and maintain listening devices—even to snoop on their own relatives.

I find it extraordinary that, at a time when our government can no longer draft men into the armed forces, Congress would allow it to conscript them into its spy corps. Even General Gage, who quartered his troops in private homes, would not have been so bold as to compel colonists to spy for him. On the theory that any liberty has its price, the bill thoughtfully provides that the conscripted spies must be compensated "at the prevailing rate," but it says nothing about death benefits to Miami landlords who are hauled into court and ordered to betray their CIA-trained Cuban tenants.

* * * * * * *

There is much more that I could say about the bill and its lack of a firm constitutional foundation. In closing, however, I would simply like to remind the Committee of some words written by Justice Frankfurter, dissenting in *United States* v. *Rabinowitz*, 339 U.S. 56, 69 (1950):

"It is true also of journeys in the law that the place you reach depends on the direction you are taking. And so where one comes out . . . depends on where one goes in. It makes all the difference in the world whether one approaches the Fourth Amendment as the Court approached it in *Boyd* v. *United States*, . . . or one approaches it as . . . a formality. It makes all the difference in the world whether one recognizes the central fact about the Fourth Amendment, namely, that it was a safeguard against recurrence of abuses so deeply felt by the colonies as to be one of the potent causes of the Revolution, or one thinks of it as merely a requirement for a piece of paper."

The CHAIRMAN. Before we begin, let's take a minute to bring the committee and the witnesses up to date on the committee's discussions with the Justice Department and the FBI regarding some of the principal issues raised by S. 1566.

As our witnesses know very well, and as this committee, I am sure will recall, though this bill was introduced this year, its predecessor was introduced in the previous session of Congress and was a product of consideration in the Judiciary Committee, and I think it is fair to say, a significant refinement as a result of this committee's activities. And the witnesses that are now seated before us played an important role in this analysis.

We owe to Attorney General Levi a vote of thanks for the efforts that he made in this regard.

The first issue involves the standard for electronic surveillance of Americans. The bill provides that a court must find probable cause that an American citizen or resident alien is an "agent of a foreign power" before he is targeted for surveillance. However, as we recall, problems arose with the definition of "agent of a foreign power." In 1976 this committee reached an agreement with Attorney General Edward Levi on a three-part definition, trying to increase the protection of American citizens and narrow the target as far as electronic surveillance was concerned.

None of us were completely happy with the standards, frankly. They were clearly a compromise. The third part did not require any indication of Federal crime. It was written very strictly so it would not allow surveillance based on a person's political activities. The first part of the standard also posed some problems because the term "clandestine intelligence activities" was so nebulous. "Clandestine intelligence activities" could include not only espionage and other forms of spying,

but also political activities on behalf of any foreign power. The way the standard was written, we could not rule out the possibility of surveillance of Americans whose political efforts on behalf of a foreign government might be labeled clandestine and who might be considered likely sometime in the indefinite future to violate the broad Foreign Agents Registration Act.

We are not talking about the obvious spy and saboteur, espionage activity in a relationship with a foreign government. We are talking about an American citizen who shares a similar concern for the interests of another country and engages in legitimate expression in the political process to get this country to follow certain procedures. We are all familiar with the strong ethnic ties many Americans have that increase their sensitivity as far as world problems, and particularly regional and other nation problems.

We recognized these problems in 1976, and we were willing to accept them for the sake of reaching agreement on the bill. However, we were concerned about any noncriminal standard for wiretaps or bugs, no matter how tightly written. Last July Attorney General Bell told us that it was almost equivalent to a criminal standard, and although I was concerned about the lack of a criminal standard, I think by any assessment, the bill after it came out of this committee, was in much better shape in this regard than the one that came out of the Judiciary Committee in 1976.

But in the interim, this last year, we have been working to try to deal with this problem, working with the Justice Department, the FBI, as well as interested citizens such as those present here today, and others, to reconsider the definition of agent of a foreign power.

With this in mind, I intend to join with others who may be similarly concerned about this problem in offering an amendment. The definition of "agent of a foreign power" which would read as follows: "(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." I want to emphasize, "may involve a violation of the criminal statutes of the United States."

Also, "(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;" or in addition "(iii) is or may be knowingly engaged in sabotage or terrorism or activities in furtherance thereof, for or on behalf of a foreign power."

The conspiracy standard would be retained, but we will make clear that the conspirator must meet all the "knowingly" requirements of the other standards. Another provision may be added to say that no American should be surveilled solely on the basis of activities protected by the first amendment.

This definition eliminates the noncriminal standard, and provides new safeguards against unjustified surveillance of political activities. The standard for clandestine political activities requires proof of direction by an intelligence service or network and an imminent criminal violation. On the other hand, the Government has somewhat more leeway to protect against clandestine intelligence gathering activities, that

is, spying, which may involve a Federal crime, as well as persons who may be engaged in sabotage or terrorism, which is a matter of great concern to us.

I will say to you just briefly before yielding, as a civil libertarian I am still not totally satisfied with two or three words in that compromise or that amended language. As one who feels that we have a dual responsibility not only to protect the civil liberties of American citizens but also to protect our country and to give our governmental agencies the tools they need to legitimately, legally, let me emphasize legitimately and legally, protect the rights of all of us from those who would take away our freedoms, I think in the exercise of both of those responsibilities, this is about as close as we are going to come.

I want to salute all of those and thank all of those who have worked on this language. I hope they will share my feeling that we are not wed to every dot and every title. We are anxious to have an examination by those who may not be as familiar with it as we are and also who may possess a broader experience of the impact of the wording, of the intention in the language.

On a separate issue, the surveillance of Americans abroad, we will introduce legislation tomorrow. My distinguished colleague from Kentucky, Senator Huddleston, has been laboring mightily in this regard. We are going to introduce those charters tomorrow, and in this legislation will be requirements of a court order for all electronic or signals intelligence activities targeted against Americans abroad. This bill will be part of the committee's intelligence charter legislation covering the CIA, the National Security Agency, and any other intelligence agency that may conduct surveillance abroad.

We have decided that overseas surveillance should be dealt with in charter legislation, along with similar techniques like physical searches and mail opening. We will be taking up S. 1566 separately, and we hope to report it to the Senate floor in the near future. Electronic surveillance abroad, dealing with the subject of the hearing process, give and take where everyone who will be affected will have a chance to be heard so we can decide to see whether those provisions actually do what we need to do to fulfill the dual responsibility that we have.

In closing, I think it is fair to say we have made significant progress in our consideration of S. 1566, and we are interested in other issues besides the criminal standard. We hope we can resolve these issues promptly so the bill can be enacted into law this year, because I think it will be the most significant step we can take in a relatively short period of time to begin the rebuilding of confidence in our agencies and in our political system.

I yield to the distinguished Senator from Kentucky.

Senator HUDDLESTON. Thank you, Mr. Chairman.

In the interest of time, and since our witnesses have already been waiting for a period, I would ask unanimous consent to submit into the record an opening statement and just say that I am pleased that we are back on the track in the development of this legislation, the need for which I think has been amply demonstrated. I think that enactment with the proper refinements, of the bill that is before us and, hopefully, of the charter legislation that will be introduced by the committee tommorrow, will have brought us a long, long way toward

the protection of our rights and liberties in this country and toward the more constitutional operation of all of our intelligence agencies. At the same time we will have established a framework within which those agencies can operate efficiently and effectively and provide us with the intelligence that our country needs.

I am hopeful that we can proceed without delay on all of these activities, giving ample time, of course, for the necessary refinements and modifications that may have to be made.

Thank you very much, Mr. Chairman.

[The prepared statement of Senator Huddleston follows:]

PREPARED STATEMENT OF HON. WALTER D. HUDDLESTON, U.S. SENATOR FROM THE STATE OF KENTUCKY

I am certain that everyone is pleased that we will soon reach the end of our quest for legislation to curtail and control the use of electronic surveillance techniques for intelligence purposes by federal agencies. The misuse of the surveillance techniques was well documented by the original Select Committee on Intelligence, and there is no doubt in my mind that this legislation is urgently needed. However, in case some of our memories on the subject have dimmed with the passage of time, I will quote one paragraph from the findings of the Committee which states very succinctly why this legislation is needed.

"These intrusive techniques by their very nature invaded the private communications and activities both of the individuals they were directed against and of the persons with whom the target communicated or associated. Consequently, they provided the means by which all types of information—including personal and political information totally unrelated to any legitimate governmental objective—were collected and in some cases disseminated to the highest levels of the government."

I believe that we need a strong bill which will assure that an individual's privacy will not be unnecessarily invaded through the use of these techniques or that his or her rights will not be ignored by federal agents doing what they arbitrarily consider to be in the best interest of national security. The Constitution guarantees individuals in this country certain rights, and it is the duty of Congress to protect these rights from intrusion either from within or without.

S. 1566 has been the subject of a long and protracted debate and is a much better bill than S. 3197 because of this debate. However, there is still room for improvement, and I will support all appropriate efforts to tighten further some of the provisions of the bill to assure that the abuses of the past do not return to haunt us in the future.

I commend all the parties who have been involved in refining and shaping this bill. The members and staff of both the Intelligence and Judiciary Committees have devoted many long hours to this bill and deserve a great deal of credit for their efforts.

The spirit of compromise, which is absolutely necessary to produce a controversial piece of legislation such as this, has been exemplary. As the distinguished Chairman indicated, there is tentative agreement on eliminating the non-criminal standard in the bill, which has been a major stumbling block. I support this effort to improve the bill, although I still am concerned about the vagueness of some of the proposed language.

I am certain that the witnesses we have before us today will have important recommendations to make, and I can assure them that I will be listening with an open mind.

The CHAIRMAN. Senator Case?

Senator CASE. Thank you, Mr. Chairman.

I shan't take any time at all. I concur with your remarks, Mr. Chairman, and those that the Senator from Kentucky has made. A lot of hard work has been put in on this by a great many people, including many of my colleagues. I appreciate this and I am anxious to get the hearing under way so that we can hear from concerned people about this very difficult and I would almost say tricky subject.

Thank you, Mr. Chairman.

The CHAIRMAN. The Senator from Indiana.

Senator LUGAR. Mr. Chairman, I would join you and our colleagues on this committee in welcoming this hearing for additional refinement on this legislation. I think it is an important bill and I appreciate the two factors, Mr. Chairman, that you brought forward in your statement. We have a tremendous obligation to protect civil liberties in this country and a tremendous obligation in terms of obtaining intelligence, and these two are not necessarily incompatible, and I think it is important in this hearing to refine this bill, and I look forward to its early reporting and passing.

The CHAIRMAN. Thank you very much.

Gentlemen, you are familiar with why we are here. The ball is in your court.

TESTIMONY OF JOHN SHATTUCK, DIRECTOR, WASHINGTON OFFICE, AMERICAN CIVIL LIBERTIES UNION; JERRY J. BERMAN, LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION; AND MORTON HALPERIN, CENTER FOR NATIONAL SECURITY STUDIES

Mr. SHATTUCK. Thank you, Mr. Chairman. I would like to start by recognizing that I have the privilege, I believe, of being the first witness before you, Mr. Chairman, in your new position as chairman of this distinguished committee, and to congratulate you on your elevation to that position and say that we are delighted to be working with you and hope to work closely with you on this and other matters in the months ahead.

The CHAIRMAN. We look forward to that kind of working arrangement.

Mr. SHATTUCK. Thank you.

I have a statement, Mr. Chairman, that Mr. Berman and I submitted to the House Intelligence Committee approximately 3 weeks ago, and we have made it available to this committee, and I would like to ask consent that it be admitted in the record.

[The prepared statement of Mr. Shattuck and Mr. Berman follows:]

PREPARED STATEMENT OF JOHN H. F. SHATTUCK, DIRECTOR, WASHINGTON OFFICE AND JERRY J. BERMAN, LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION

Mr. Chairman: We welcome this opportunity to testify before this Committee on legislative proposals to control electronic surveillance for foreign intelligence purposes. It is a matter of obvious importance to the nation and one of vital concern to the members of the American Civil Liberties Union, a nationwide, nonpartisan organization devoted to protecting individual rights and liberties guaranteed by the Constitution.

This legislation has been proposed for the same reasons that this new Intelligence Committee was constituted: the recognition, in the wake of Watergate and revelations of massive illegal programs conducted by the FBI, CIA, NSA and other U.S. intelligence agencies, that the Congress must exercise meaningful oversight and control of the intelligence community and enact legislation and charters for the agencies which insure that intelligence activities will no longer violate the civil and constitutional rights of Americans.

The enactment of legislation to prohibit warrantless and overbroad electronic surveillance would be a major step toward reform and would signify a resolve on the part of Congress to bring our intelligence agencies under the rule of law. Legislation setting forth a strict and narrow standard for the use of this most intrusive investigative technique would afford protection for the First and

Fourth Amendment rights of citizens and would set a positive precedent for legislation defining the general investigative authority of U.S. intelligence agencies and the circumstances under which they may use other covert investigative techniques such as the search of private records and the use of informants.

We stress the interrelationship between wiretapping legislation and the proposed charters to emphasize at the outset that the Committee cannot view these bills in isolation. Whatever investigative standard is approved in the wiretap area will be a significant precedent with far-reaching ramifications. If Congress enacts wiretapping legislation with an overbroad or indefinite standard for employing this most intrusive of all investigative techniques, intelligence agencies will inevitably continue to violate the First and Fourth Amendment rights of citizens in a wide range of investigative areas. It is only logical that future charter legislation, governing the use of less intrusive covert techniques, will build on this precedent. This could result in broad investigative authority to conduct surveillance of political activity. If the wiretap standard is too low, Congress could end up authorizing rather than curtailing intelligence agency abuses.

THE CENTRAL ISSUE: THE CRIMINAL STANDARD

While four bills are under consideration by this Committee—H.R. 5632, H.R. 5794, H.R. 7308 and H.R. 9745—we will focus on H.R. 7308, the Administration proposal introduced on May 18, 1977 in both the House and Senate (S. 1566).

Before we discuss our central objection to H.R. 7308 as presently drafted—its failure to set forth a criminal standard as the basis for all national security electronic surveillance and to restrict the application of this standard to serious crimes affecting national security—we want to commend certain features of the bill, particularly

Its specificity as to the showing the Government must make to obtain a warrantless national security wiretap;

Its requirement that all such wiretaps be conducted pursuant to a judicial warrant, making it clearly preferable to H.R. 9745 which permits warrantless electronic surveillance; and

Its specificity as to the showing the Government must make to obtain a warrant to conduct electronic surveillance for foreign intelligence purposes.

Despite the positive aspects of the bill, which we strongly encourage the Committee to retain, H.R. 7308 is seriously flawed because it permits the Government to target persons for electronic surveillance without probable cause—or even a reasonable suspicion—to believe they are engaged in crime. Accordingly, we oppose the bill in its current form because we believe its low investigative standard would invite abuse and would be a dangerous precedent for future intelligence legislation.

THE NON-CRIMINAL STANDARD IN H.R. 7308

Before discussing the investigative standard for wiretapping which we believe is minimally necessary to satisfy the Constitution and curtail abuse, let us look at who could be routinely wiretapped under H.R. 7308. The bill authorizes continuous surveillance for three months or more of at least four classes of people who are not even reasonably suspected of engaging in criminal activity.

First, the bill permits surveillance of officers or employees of a foreign power without any showing 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. In the absence of any definition of "clandestine intelligence activities," there are no safeguards to protect innocent foreign businessmen, visiting foreign relatives, tourists, or any other foreign visitors to the United States from becoming the targets of "intelligence" wiretapping.

The third category of persons covered by the non-criminal standard 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 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 non-criminal standard in H.R. 7308 would 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 H.R. 7308.

A CRIMINAL STANDARD: THE MINIMUM CONSTITUTIONAL REQUIREMENT FOR WIRETAPS

Why is it so important to limit the wiretapping authorized by H.R. 7308 to a "criminal standard"? 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 H.R. 7308—a wiretap search inevitably has a dragnet effect which strains the Fourth Amendment to the breaking point. As Justice Brandeis warned in *Olmstead* v. *United States*, 277 U.S. 438, 473 (1928), "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 invasion of private speech and thought with almost no parallel.

Since wiretaps are inherently so intrusive, the ACLU has long maintained that they cannot be conducted at all without violating the Fourth Amendment. If this violation is to be minimized, no surveillance should be permitted unless a judicial warrant has been issued based upon probable cause to believe that the person to be tapped is engaged in crime. See *Katz* v. *United States*, 389 U.S. 347 (1967).

Those who seek to justify a departure from the criminal standard for "intelligence wiretaps" 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 two leading administrative search cases. *Camara* v. *Municipal Court*, 387 U.S. 523 (1967) and *See* v. *Seattle*, 387 U.S. 541 (1967). In these cases the Court sanctioned the use of area warrants for municipal authorities to conduct inspections for housing code violations, not upon probable cause of a particular housing code violation, 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. These cases did not involve a deliberate search for specific information, as does H.R. 7308. The searches were part of a general regulatory scheme to protect public health and safety. 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." *Marcus* v. *Search Warrant*, 367 U.S. 717, 724 (1961). See also *United States* v. *United States District Court*, 407 U.S. 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 particular facility.

The degree of intrusiveness 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 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 one of the premises of H.R. 7308. There is little basis for it in constitutional law.

The Fourth Amendment, of course, refers not to the rights of citizens or residents, but to 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 Amendment 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 established that an alien could invoke the exclusionary rule in a deportation proceeding. *United States ex rel. Bilokumsky* v. *Tod*, 263 U.S. 149 (1923). The extension of full Fourth Amendment protection to foreign nationals has been long 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 was noted by the Supreme Court in *Abel* v. *United States*, 362 U.S. 217 (1960). *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 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 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 like the one conducted in *Abel* 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 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. See *Alameida-Sanchez* v. *United States*, 413 U.S. 266 (1973).

Even the argument that foreign power embassies and employees—as distinguished from a larger class of foreign visitors—can be subjected to broad surveillance is lacking in constitutional support and contrary to international law. There is little basis in Supreme Court case law for a distinction between types of foreigners lawfully in the United States. Moreover, 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, their furnishings and other property thereon and the means of transport of the mission shall be *immune from search*, requisition, attachment or execution. [emphasis added.]

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 H.R. 7308 would permit. In considering the distinctions which the bill attempts to make between classes of foreigners lawfully in the United States, 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).

SHOULD CONGRESS CREATE A NATIONAL SECURITY EXCEPTION TO THE CRIMINAL STANDARD FOR WIRETAPPING

Even if the Constitution were to permit a "foreign intelligence" exception to the criminal standard for wiretapping, the question would remain: Should Congress create such an exception? This question has been answered unequivocably in the negative by the Senate Select Committee on Intelligence Activities (the "Church Committee") and by Vice-President Mondale both at the time he was a member of the Church Committee and as recently as last August in an address before the American Bar Association. Furthermore, no evidence has been offered in the Senate hearings on S. 1566, the counterpart to H.R. 7308, to justify any departure from the criminal standard, and Senator Kennedy, a principal sponsor of S. 1566, has repeatedly expressed reservations about the bill's proposed exception to the criminal standard.

The Church Committee carefully reviewed the problem of national security wiretapping and reached the conclusion that "no American be targetted for electronic surveillance *except upon a judicial finding of probable criminal activity.*" *Intelligence Activities and the Rights 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. (1976), at 325 [emphasis added]. The extraordinary degree to which national security wiretaps have been misused for political purposes was well documented by the Committee and has been further demonstrated through successful litigation. *See, e.g., Zweibon* v. *Mitchell*, 170 U.S. App. D.C. 1, 516 F. 2d 594 (D.C. Cir. 1975); *Halperin* v. *Kissinger*, 424 F. Supp. 838 (D.D.C. 1976); *Berlin Democratic Club* v. *Rumsfeld*, 410 F. Supp. 144 (D.D.C. 1976). In light of this history of wiretap abuses, the Church Committee concluded that if the existing criminal standard for wiretaps

should prove to be too restrictive "to cover modern forms of industrial, technological or economic espionage not now prohibited," then the criminal laws should be amended rather than create a new dangerous basis for intrusive surveillance." Bk. II, at 326.

The rationale for the Church Committee's conclusion was incisively expressed by then-Senator Walter Mondale when he testified in July 1976 in opposition to the non-criminal standard in S. 3197, the predecessor to H.R. 7308:

"[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 [see] 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 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.

As Vice President, Mr. Mondale reaffirmed his position on the importance of the criminal standard in a speech before the American Bar Association on August 5, 1977. The Vice President's statement on the criminal standard issue came after the Senate Judiciary Committee hearings on S. 1566 had been completed, and in this respect it appeared to reflect an awareness within the Administration that a non-criminal exception in the bill is not necessary. In any event, the case for the exception has not been made.

The Administration has now had two opportunities to explain to Congress why a non-criminal standard is necessary. Neither occasion has produced any persuasive reasons why legitimate foreign intelligence investigations would be hampered by compliance with a criminal standard. As Senator Kennedy pointed out at the conclusion of the Senate Judiciary Committee hearings on S. 1566, the Administration witnesses did not meet their burden of proof. Hearings on S. 1566 before the Committee on the Judiciary, U.S. Senate, 95th Cong., 1st Sess., June 14, 1977 [hereafter "Judiciary Hearings"]. No additional evidence to support the exception was offered at hearings conducted subsequently by the Subcommittee on Intelligence and the Rights of Americans of the Senate Select Committee on Intelligence.

Both Defense Secretary Harold Brown and CIA Director Stansfield Turner conceded before the Judiciary Committee that their agencies do not require authority to wiretap American citizens or foreign visitors not engaged in crime. As Secretary Brown put it, "the non-criminal standard is principally an FBI requirement rather than a DOD requirement." This position was repeated at the Intelligence Committee hearings. Admiral Turner noted that any non-criminal surveillance the CIA would conduct would principally be directed against foreign powers and not against individuals. Hearings on S. 1566 before the Subcommittee on Intelligence and Rights of Americans, Select Committee on Intelligence, U.S. Senate, 95th Cong., 1st Sess., July 21, 1977 (unpublished) [hereinafter "Intelligence Hearings"].

The arguments for the inclusion of a non-criminal standard in S. 1566 and H.R. 7308 have come from the Department of Justice. Attorney General Griffin Bell at first suggested to the Judiciary Committee that a less stringent standard was needed for the investigation of foreign visitors (although the Ford Administration had decided it was *not* needed the year before) because of an increase in the number of "communist-bloc officials" travelling to the United States. But when asked by Senator Kennedy what specifically had changed in one year "in terms of the nature of the threat," the Attorney General could only suggest that "maybe you're dealing with a different set of people." Judiciary Hearings. This assertion was not repeated in the subsequent hearings, although Senator Kennedy had invited the Department to attempt to show whether there was "an additional threat . . . to our security interests" that would warrant broader investigatory authority.

Turning to the question of why it is necessary to authorize wiretaps on American citizens and resident aliens not engaged in crime, the Justice Department witnesses took the position that "the current espionage laws are not yet complete enough and clear enough to . . . reach all forms of espionage that need to be covered". They asserted that the "national defense" interests protected by

the espionage laws are narrower than the "national security" interests protected by H.R. 7308. As several other witneses pointed out, however, the Supreme Court in the leading espionage case of *Gorin v. United States*, 312 U.S. 19, 28 (1941) has construed the terms "national defense" and "national security" to have similar meanings for a judge considering whether to issue a warrant. This point was brought out by the Attorney General himself, who stated in response to a request for an explanation of the supposed distinction between "national defense" and "national security": I don't know if I can give you any more, other than to say: "National Security to me is broader than national defense". Judiciary Hearings.

This is the extent of the Administration's testimony to date relating to the need for a non-criminal standard in H.R. 7308. Following the Senate Judiciary Committee hearings on S. 1566, Attorney General Bell sent a letter to the Committee responding to certain written questions. In this letter the Attorney General amplified his testimony by describing six hypothetical cases in which he asserted the government would be authorized to conduct a wiretap under S. 1566, but not under the espionage laws. It is evident, however, that the espionage laws would be sufficient to authorize a wiretap in each case where it would also be authorized under the non-criminal standard in S. 1566 and H.R. 7308.

THE APPROPRIATE STANDARD FOR H.R. 7308

H.R. 7308 should reflect the fundamental principle that no persons protected by the Constitution should be subjected to intrusive surveillance unless there is evidence that they are engaged in serious criminal conduct. Otherwise they should be left alone. In the context of national security, no persons should be targetted for electronic surveillance unless the Government has evidence they are engaging in criminal conduct which directly threatens national security. To bring H.R. 7308 in line with this principle, we recommend the following alternatives:

1. Amend or Omit the Non-Criminal Standard for Americans

The non-criminal definition of "agent of a foreign power," Section 2521(2)(B)(iii), should either be amended to reflect a criminal standard or omitted from the bill. To accomplish this, we call the Committee's attention to a proposed amendment to the companion bill, S. 1566, which would add "likely to violate the criminal statutes of the United States" to this subsection. Alternatively, we refer to the recommendation of the Church Committee which calls for the omission of any non-criminal standard with the understanding that if certain conduct is considered dangerous to national security but not violative of the laws of the United States, amendment of the espionage laws should be considered. In any event, Congress should not set a dangerous precedent by authorizing the wiretapping of persons engaged in *lawful* conduct.

As we have pointed out, the Government has not met its burden of proof that this subsection is warranted. On the other hand, the government has interpreted this section far too broadly in arguing that *all of the hypothetical* cases can be reached under this standard. In either case this argues for deletion or amendment.

2. Amend the Criminal Definition of Agent of a Foreign Power Applicable to Americans

The criminal definition of "agent of a foreign power," 2421(B)(i) should be tightened considerably. First, to insure that the Government does not wiretap any Americans based on the speculation that they may one day in the indefinite future violate the law, the words "will involve" should be modified by the word "soon." More important, the section should be amended to insure that it will be invoked only when there is evidence of a crime directly affecting national security.

In the bill as introduced, the term "clandestine intelligence activities" is not defined and evidence of any criminal law violation can trigger a wiretap. Without specific definition, clandestine intelligence activity could be interpreted to mean any form of private political activity, including attending meetings or lobbying. It could apply to planning a demonstration against our involvement in a foreign conflict (like the Vietnam War) or lobbying for arms to Israel. Arguably, if picketing without a permit or civil disobedience were planned, persons engaging in these activities could be wiretapped. While this may seem far-fetched, we must remember that OPERATION CHAOS, COINTELPRO, and the NSA cable intercept programs were all based on such interpretations of "counterintelligence."

To avoid abuse, we believe that Congress should narrowly define "clandestine intelligence activity" in the bill and see that it reflects activity which amounts

to evidence of possible espionage. In addition, Congress should specify in the subsection those national security crimes or related offenses which are proper concerns for counterintelligence investigative agencies—for example, those crimes listed in Section 2516(1)(a) of the Omnibus Crime Control and Safe Streets Act having to do with national security.[1] In other words, the principle followed by Congress in Title III of the Safe Streets Act that all crimes do not warrant wiretapping should be followed in this legislation as well, since it would deter the government from engaging in overbroad surveillance. For example, to include the vague Foreign Agents Registration Act as a possible basis for wiretapping can result in extensive surveillance of lawful political activity and association. Enumeration of crimes would avoid this problem.

We emphasize that in the long history of executive authorization of national security wiretapping dating back to the 1940 order of President Roosevelt, the Executive branch has always specified that wiretapping could only be conducted when there was evidence of espionage, treason, sabotage, or violations of the neutrality laws. See Warrantless FBI Electronic Surveillance, in *Book III, Final Report* of the Select Committee to Study Governmental Operations with respect to Intelligence Activities, 94th Congress, 2d Sess. Report No. 94–755. If Congress intends to reform intelligence activities, it would be unconscionable to authorize even broader surveillance than was permitted by executive order in the past.

3. Amend the Conspiracy Sections Applicable to Americans

As we pointed out earlier, the conspiracy section of 2521(2) is far too broad. If the non-criminal standard remains in the bill, the conspiracy section should not apply to this subsection. A conspiracy to aid and abet others in what is by definition lawful conduct is two steps removed from criminal activity. As applied to criminal conduct, subsection 2521(B)(2)(iv) must be changed to cover only those who knowingly aid or abet any person whom they know to be engaged in activities described in the section. As presently drafted, a person could aid or abet a person in lawful activities and be wiretapped because the person is engaged in some other possible illegal or non-criminal "clandestine intelligence" activity.

4. Amend Definitions of Agent of a Foreign Power Applicable to Foreigners and Visitors

Employees of a foreign government in the United States should not be subjected to wiretapping simply because of their status, and there should be no separate standard for foreign visitors and students. We believe that with adequate definition of "clandestine intelligence activities" and a clear relationship between such activities and national security crimes, the government will have sufficient authority to protect vital national security interests. The Constitution requires no less. Moreover, if we are to get at the problem of massive surveillance by foreign governments of the communications of United States citizens, we must not ourselves engage in similar sweeping surveillance.

In our testimony today, we have focused on the critical issue presented by this legislation. However, in an attached appendix we suggest other important amendments that must be made in H.R. 7308, having to do with the procedure for approving wiretap authorizations, obtaining judicial certification for electronic surveillance, permitting a judge to go behind a certification, and insuring that intercepted conversations are minimized. We here call your attention to these important amendments and again reiterate our concern about the overbroad investigative standard in the current draft.

Under our constitutional system the wiretapping of persons who are engaged in lawful activity has no place. Moreover, in legislating controls over wiretapping, Congress must not set a precedent for legislated charters that would authorize continued intrusive surveillance of political activity by U.S. intelligence agencies.

ADDITIONAL AMENDMENTS

1. § 2521(b)(6)(C) should be amended to declare 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.

[1] This is the underlying concept of H.R. 5632, which we endorse.

2. § 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; or (b) 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 surveillance of foreign powers. The minimization procedures in § 2521(b)(8) do not require minimization of surveillances directed at non-U.S. persons. Information acquired about a U.S. person can be stored so that it is routinely retrievable under the person's name. The amendment is intended to protect U.S. persons against such routine storage and retrieval practices.

3. § 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 should be an essential element in the legislative scheme of H.R. 7308, 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."

4. § 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.

5. § 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), the certification or certifications are not arbitrary or capricious, and a judicial finding has been made that the certification or certifications are correct on the basis of the statement made under section 2524(a)(7)(E)."

Comments.—One of the principal new features of H.R. 7308 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 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.

6. § 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.

7. § 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 wiretaps. 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.

8. § 2525(c) should be amended to eliminate the one year authorization period for foreign power surveillance and limit all authorizations to ninety days.

Comments.—The extraordinary intrusions permitted by this bill are dramatically demonstrated in the provision authorizing surveillance of foreign power

without review for one year periods. The ninety day periods permitted for United States persons are already far beyond the limits of Fourth Amendment reasonableness.

9. § 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.

10. § 2527 should be amended to add the following at the end:

"(c) 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 preceding year."

Comment.—These important reporting provisions were contained in S. 3197 and should be reinstated in H.R. 7308 and S. 1566.

11. § 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 surveillance. Common law warrants which do not follow the procedures of this legislation should not be permitted to authorize any surveillance.

12. 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 wiretapping 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).

APPENDIX

The Justice Department Hypotheticals

In response to questions posed by Senator James Abourezk, Attorney General Griffin Bell sent a letter to the Senate Judiciary Committee wherein he outlined six hypothetical cases which Justice Department officials contend warrant a departure from a criminal standard in the Foreign Intelligence Surveillance Act of 1977. According to the Justice Department, these cases could not be reached under current espionage laws. After studying the cases, it is our contention that in three of the cases outlined, a judge would issue a warrant under current espionage laws and that in the remaining three cases, a judge would not issue a warrant even under S. 1566 as currently drafted. In sum, the Administration has not made a case for departing from the criminal standard in this Act.

Case No. 1

"A *Spinelli-qualified*[2] informant reports that A has, pursuant to a foreign intelligence service's direction, collected and transmitted sensitive economic information concerning IBM trade secrets and advanced technological research which ultimately would have a variety of uses including possible use in a sophisticated weapons system, but which is not done pursuant to a government contract. A is placed under physical surveillance and is seen to fill dead drops which are cleared by a member of a Communist bloc embassy suspected of being an agent of its foreign intelligence service."

Comment.—This case turns on whether commercial information such as an IBM trade secret which might be used in a sophisticated weapons system constitutes "national defense" information or information "relating" to the national defense under 18 U.S.C. 794. The Justice Department contends that it may not. However, the Supreme Court, in *Gorin* v. *U.S.* 312 U.S. 18 (1941), stated: "National defense . . . is a 'generic concept of broad connotations, referring to the military and naval establishments and the related activities of military and naval establishments and the related activities of national preparedness.' We agree that the words 'national defense' in the espionage act carry that meaning." *Id.* at 28. Thus, if a court found that a person fit all of the other criteria of 2421(b)(2)(B) and that the information being gathered was from an industrial source, it still would have no difficulty finding that there was probable cause to believe that 18 U.S. 794 was being violated.

Case No. 2

"Pursuant to the physical surveillance of a known foreign intelligence officer, B is seen to clear dead drops filled by that officer. On the second Tuesday of every month B drives by the officer's residence, after engaging in driving maneuvers intended to shake any surveillance. Within 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 employee of the opposite sex specializing on matters dealing with the country of the intelligence agent."

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

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

Case No. 3

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

Comment.—This case, like Case Number One, turns on the meaning of "national defense" and "related" information in current espionage law. Nothing in Section 793 of Title 18 limits such information to data that is classified or developed pursuant to contract. Again, given the Court's broad reading in Gorin, the "valuable information concerning components which are used in United

[2] *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.

States weapons systems" would be covered under 18 U.S.C. 794. Since all the other elements under 2521(b)(2)(B) have been met, there would be probable cause to find that a conspiracy to violate Section 794 of Title 18 existed.

Case No. 4

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

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

Case No. 5

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

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

Case No. 6

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

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

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

Mr. SHATTUCK. I will summarize a number of points in that statement, and try to give some overall perspective to the importance of the legislation before this committee which is extremely important to civil libertarians in the Senate and to the country. The wiretap legislation before you has been proposed, we believe, for the same reason that this committee was constituted, and that is the Congress must exercise

meaningful oversight over the intelligence community to insure that intelligence activities will no longer violate the civil and constitutional rights of citizens. We have a long and somewhat tortuous history in recent years of disclosures of these intelligence violations, and we are pleased that this committee is now seeking to put those abuses behind us.

The enactment of a bill to prohibit warrantless and overbroad electronic surveillance would be a major step toward intelligence reform and would signify a resolve on the part of Congress to bring our intelligence agencies under the rule of law.

We believe that legislation setting forth a strict and narrow standard for this most intrusive of all investigative techniques would protect the first and fourth amendment rights of citizens, and would set a positive precedent—and for charters defining the general investigative authority of the intelligence agencies. It is important for us all to understand, Mr. Chairman, as you yourself so well understand, that the wiretapping legislation and the proposed charters are very closely related, inevitably so. Whatever investigative standard is approved in the wiretap area will be a significant precedent, with far-reaching ramifications as the committee moves ahead in the charter field.

If Congress enacts a wiretap bill with an overbroad or indefinite standard, or a standard that does not link investigative activity to the investigation of crime, the intelligence agencies, we fear, will continue to violate the first and fourth amendment rights of citizens in a wide range of other investigative areas. In other words, if the wiretap standard is too low, Congress could end up authorizing rather than curtailing many of the abuses that have come to light in recent years.

The American Civil Liberties Union position on wiretapping is well known, and that is that the very conduct of wiretapping necessarily strains the fourth amendment which protects us against unreasonable searches and seizures, to the breaking point. Wiretaps are so intrusive that all conversations are picked up over a period of time, which means that a wiretap is very difficult to minimize in terms of the scope of the search and seizure that is conducted.

This is why—in addition to the precedent that this legislation will set for the future of legislation to control the intelligence agencies—this is why the criminal standard is so important to this bill.

Now, the criminal standard, as your opening remarks, Mr. Chairman, suggested, is a very complicated issue. There are many elements in the issue; for example, four classes of persons now in the legislation, prior to any introduction of amendments, can be wiretapped without any reasonable suspicion or probable cause that they are engaged in criminal activities. These include foreign powers, foreign visitors, businessmen, students, other people coming and visiting this country, U.S. persons, and conspirators or persons who aid or abet persons in those other three categories.

Now, we are deeply concerned about all of those categories, Mr. Chairman. I think that what we have heard this morning indicates that the committee is equally concerned about many of those areas. We are concerned about the interception of first amendment information—information about the political activities of a person—and I think that the chairman has indicated an equal concern with that by supporting the inclusion in this bill of a provision that would make it clear that even if we go to a criminal standard, there will be no author-

ization of interceptions of information protected by the first amendment.

The tightness of the definitions is also very important to us. The clandestine intelligence activity definition which has yet to emerge in the course of these hearings is one example. There are many concerns, in other words, and I think instead of going into each of them in detail, we would prefer to open ourselves to questions by members of the committee.

We are, of course, also interested in improving the bill, as the chairman has indicated, in other areas, apart from the standard to be used with respect to the investigations that would be permitted.

So without further comment on the opening statement you made, Mr. Chairman, we are prepared to proceed to answer any questions that you might have.

The CHAIRMAN. Are you familiar with the language of the proposed amendment, and if so, would you give us your critique of its strengths and weaknesses, please?

Mr. SHATTUCK. I think I will turn the microphone over to Dr. Halperin.

The CHAIRMAN. Who has had some significant personal experience in this field.

Mr. HALPERIN. First of all, I try not to let that get in the way of my position. I think the elimination of the old paragraph (3) which involved the so-called noncriminal standard is clearly a substantial step forward. The section 1, which in effect is a substitute for the old section 3, clearly links now any surveillance of persons believed to be engaged in clandestine intelligence collection to a criminal standard. I think that is a step forward.

The additional provisions in the new paragraph (2) do provide additional requirements in relation to other clandestine intelligence activities. I think we would prefer to limit the bill simply to clandestine intelligence gathering, but these additional provisions to tighten and provide additional protection, particularly if there is provision which your statement suggests, which may be added to the bill, which we think is absolutely essential; that is, a provision saying that no person can be the subject of surveillance solely on the basis of first amendment protected activities.

So whatever the definition of other clandestine intelligence activity, it cannot include a person who is simply engaging in activities which are protected by the first amendment of the Constitution. I think that provision is essential in connection with 1 and 2 to make it clear that political activity protected by the first amendment cannot be the sole basis for wiretapping somebody.

Now, paragraph 3 raises some additional problems because what it does is to move terrorism and sabotage to a reasonable suspicion standard rather than a probable cause standard, and I think clearly we would prefer, would still prefer to have that provision left the way it was in terms of requiring probable cause.

If——

The CHAIRMAN. Excuse me for interrupting, but I am sure you are aware that I much prefer the probable cause standard, but what we are trying to do is see if there is room for a tradeoff which could deal with terrorism before the deed is performed.

Mr. HALPERIN. The argument as I understand it is that this provision should be parallel with 1, relating to conventional intelligence activities. I think that the problem is that the way it was drafted—and I think this is probably just a drafting problem—it is not parallel because section 1 requires that you be engaged in the present in what is called clandestine intelligence activities. The only thing that is uncertain or may be in the future is whether it will involve a violation of the criminal statutes, so that it says knowingly engages in clandestine intelligence activities, which activities involve or may involve a violation. But the way section 3 is drafted it does not require any current activity at all because it says is or may be knowingly engaged or sabotage or terrorism or activities in furtherance thereof. So there need be no current activity at all because they simply could find that you may be in the future engaged in activities in furtherance of terrorism.

The CHAIRMAN. So you are concerned about "may" being defined as a matter of time, not as a matter of a certainty.

Mr. HALPERIN. Right.

The CHAIRMAN. I think that is a fair assessment.

Mr. HALPERIN. It is important that it be rewritten so that it parallels section 1, so that it says that you are engaged in activities which are, relate to, or involved in sabotage and terror which may be violations of a criminal statute, the way 1 is written. There are problems in drafting to do that, and I think this was an attempt to do that. I just think the language is not quite to the point where it accomplishes that.

The CHAIRMAN. We are glad to have some help from you as to how you might do that from that standpoint.

If we understand your concern, again, let me try to pin this down. First of all, our concern in talking about terrorism and sabotage is the loss of a large number of lives if you don't get something stopped. I am sure you concur, that because of the time factor involved, you have to act quickly, at which time you may not have sufficient facts for ordinary probable cause, but you do have good, reasonable suspicion as far as the kind of activities involved here.

Now, that is what we meant "may" to mean, not "may" sometime in the future.

Now, you are concerned that the "may" could involve almost anyone.

Mr. HALPERIN. I think we would obviously prefer to have probable cause and not have "may" at all, but leaving that aside, the concern is that the "may" relate to whether it will actually produce the terror or sabotage, as is defined in the bill, but that their activities already be underway at the time that the request for surveillance go into effect, just as some activity must be underway for clandestine intelligence gathering. It should simply be a belief that sometime in the future somebody may do something which will be in furtherance of sabotage or terror. I think we would be glad to submit language and try to work with the staff to develop language that does that.

The CHAIRMAN. May I ask this, an advance appraisal, and then I will have a chance to study it.

We'd better have a chance to make sure what we are talking about on this end before we get your reaction.

Mr. HALPERIN. I think Mr. Shattuck would like to comment on that as well, and then I would like to make two other comments related to that.

The CHAIRMAN. Please.

Mr. SHATTUCK. Also in that same section, Mr. Chairman, relating to sabotage and terrorism, we are disturbed about two other matters in addition to the standard which Mr. Halperin has been discussing. First is the definition of terrorism. It seems to us that it is appropriate, given the purpose of this bill, in guarding against foreign power activities, to define terrorism as international terrorism so that we are not talking about the investigation of domestic groups under a lower standard. Domestic groups ought to be investigated under title III. That is certainly the purpose of the title III investigation. But this is going to be a broader investigative authority, and therefore we would urge that the terrorism be amended to make it clear, as the Executive Order does, that we are talking about international, or internationally based groups and not domestic groups.

The second point that I wanted to make about that section, Mr. Chairman, was the——

The CHAIRMAN. Would you excuse me just a minute, please?

Mr. SHATTUCK. Yes.

[Pause.]

The CHAIRMAN. Excuse me. Go ahead.

Mr. SHATTUCK. The second point I wanted to make about that section concerns what we believe is really the use of a superfluous term, "in furtherance thereof"—"is or may be knowingly engaged in sabotage or terrorism or activities in furtherance thereof." In light of the conspiracy section that is already in the bill, we don't understand the purpose of the "in furtherance thereof" language, at least insofar as it has any other purpose than that which is already contemplated in the conspiracy and aiding and abetting section.

So those are two additional points we wanted to bring to your attention in this section.

The CHAIRMAN. Let us explore that. We are talking about a significant standard of involvement, not just a casual, unwitting incidental involvement.

Mr. HALPERIN. Mr. Chairman, if I can make one comment on the conspiracy provision, I think we are all agreed, but just to be sure, I think it is important that the person be aiding in the activities specified in the statute. As it is now written, literally, one could be aiding or abetting a person engaged in, say, clandestine intelligence, but not be aiding them in that, be aiding them in a lawful political activity, and I think it is just important to add a provision that makes that clear.

You say in your statement that they meet all the knowing requirements of the other standards. That doesn't quite meet the point.

The CHAIRMAN. I don't think you are familiar with the latest revision.

Mr. HALPERIN. No, I haven't seen it.

The CHAIRMAN. In which we try to deal with that by saying "knowingly aids or abets activities" described in the previous three paragraphs.

Mr. HALPERIN. That would solve it. That would do it.

Now let me just make one other point, and that concerns the foreign visitors provision of the statute, and this is a point I have made now before several other committees considering this bill.

I think it is important to find a way to limit that to the small number of countries where it is believed that they regularly and syste-

matically exploit foreign visitors to the United States for the purpose of clandestine intelligence. Mr. Kelley, in his testimony, has constantly justified this provision in relation to the large number of Russian visitors and Russian seamen who come to the United States.

As the language is now written, it could be used for Japan, France, Israel, Venezuela, or any country, and again, this is a matter that has been discussed extensively, and I would hope language could be found which limits the applicability of that provision to countries which have a record of systematically using foreign visitors for this purpose.

The CHAIRMAN. Would you be more comfortable with this language:

> * * * openly acts in the United States in the capacity of an officer or employee of a foreign power, or is a national of a foreign nation which engages in clandestine activities in the United States under circumstances that make it likely that such a person present in the United States is or may be engaged in activities against the United States.

That does narrow it down to those persons who are involved in those kinds of activities in the United States.

Mr. HALPERIN. I would want to see the language in writing, but as you read it, it sounds like a significant improvement.

Mr. SHATTUCK. Mr. Chairman, I think Mr. Berman wanted to add something to that point.

Mr. CHAIRMAN. Well, before he does, let me just point out, you might look when we get this revision to you here, at subsection (3) (iii) where we talk about sabotage or terrorism or activities in furtherance thereof, we say for or on behalf of a foreign power.

Does that deal, Mr. Shattuck, with the concern you had about domestic terrorism being covered in title III?

Mr. BERMAN. I wanted to speak to that point. There is a definition of international terrorist activity which is in the executive order issued by President Carter which makes clear that terrorism not only be for or on behalf of a foreign power, but under section 4–209(c) of the executive order, that the terrorism must transcend national boundaries in terms of the means by which it is accomplished, the civilian population, government or international organization it appears intended to coerce or intimidate, or the locale in which its perpetrators operate or seek asylum. That would seem to be more definite in terms of limiting this legislation to terrorism for or on behalf of a foreign power. We don't want a repetition of the previous situation of surveilling groups like the Communist Party USA because they allegedly were acting for or on behalf of a foreign power in some abstract sense. This would, I think, make it clear that we are talking about international terrorist activities, and second of all, make it clear that we are not in any of these sections talking about political activities. I think that it is essential for his amended language also to include the provision that no American may be surveilled because of his political activities or first amendment activities if we are not going to define clandestine intelligence activities in this legislation, or make it clear as it is drafted; I think we can at least make it clear that speech, and even provocative speech, is not included within the definition of either sabotage or terrorism or clandestine intelligence activities.

The CHAIRMAN. That is a point well taken. I mentioned that in my opening remarks. In considering it, our problem is we have it specifically included in the charters, but we were having difficulty knowing where to put it here. Let me just ask the staff to find a place

to put it. I understand that the Justice Department has no reservations about this. They are willing to accept this, and it is the kind of protection we are all concerned about.

Mr. BERMAN. We think it should be a modification or clarification of the definitional section of this bill because the minimization criteria, which Dr. Halperin will talk about, get at this problem from another angle of minimizing the dissemination of information about first amendment activity. We think that the uncertainty about overbroad definitions can be made clear by including this provision and then making clear in report language that first amendment activity is not reached by this statute.

The CHAIRMAN. I think we will examine that.

In the whole terrorism area, where would you categorize the group of American citizens who are planning and conspiring to participate in a terroristic act in this country where the leadership or a significant part of the conspiracy involves American citizens who are at that time abroad, financing it, directing it, but the activities are conducted by American citizens in the United States?

Mr. SHATTUCK. Pursuant to a foreign power, I take it. I take it you are talking about the additional qualification that would be in the bill under title III which would be pursuant to the direction of a foreign power. Certainly if it were not on behalf or directed by a foreign power, that activity would not be included within this bill, I think, and it would be necessary to proceed under title III for a criminal warrant to wiretap such a group.

Mr. BERMAN. We are trying to restrict all of these sections to a definition of agent of a foreign power that does not include American groups simply because they have some concern for people abroad, or because of their foreign policy views. I think that is not part of a counterintelligence jurisdiction.

The CHAIRMAN. Any other observations?

I have a few questions.

Senator CASE. Mr. Chairman, I think the suggestion was that we go after domestic law, and what is that?

Mr. SHATTUCK. Under title III of the Omnibus Crime Control and Safe Streets Act of 1968, the Government would have to go to a judge and show probable cause that evidence of a crime could be seized pursuant to a wiretap and have that judge then issue a warrant for a tap to be placed on that particular organization. That is the law at the moment. Certainly the Supreme Court in the *Keith* case, and further, the D.C. Circuit Court of Appeals in the *Zweibon* case, indicated that in the absence of foreign direction, financing or control of such a group, it would be essential to proceed under title III. We are very concerned that this bill not change the constitutional balance that has already been established by the Supreme Court. I think the question that Senator Bayh was asking me would suggest that in the absence of direction by a foreign power, if the bill were able to reach such a group, then there would be a basic change in the constitutional balance, and that is something we would be very concerned about.

The CHAIRMAN. Any further questions?

Senator CASE. No; I am sorry to interrupt you.

The CHAIRMAN. Senator Huddleston, do you have any questions?

Senator HUDDLESTON. No questions.

The CHAIRMAN. Senator Lugar?

Well, gentlemen, thank you very much.

Senator HUDDLESTON. I thought Dr. Halperin was going to make a comment.

The CHAIRMAN. Well, I was going to say I was going to be sending questions on minimization. You might want to deal with that here while you are here.

Mr. HALPERIN. I would like to comment on two other provisions of the statute, or perhaps three. One has to do with minimization in the form of indexing, and it is a problem of whether or not the FBI can maintain indexes of the names of American citizens which will enable it to retrieve information from these electronic surveillances by looking up the records of American citizens.

Now, we know that this has been one of the forms of abuse in the past. Presidents have asked the FBI what it knew about the views of U.S. Senators, for example, on the Vietnam war. The Bureau then was able by the indexing it maintained to discover if any U.S. Senators talked to foreign embassies on the phone, that the views were then obtained, and that that information was then provided to the White House, both in the Johnson and Nixon administrations.

The bill as it is now written prohibits the indexing of information under the name of an American citizen if that information, it says on page 9, "relates solely to the conduct of foreign affairs," and therefore I think it clearly contemplates that information will be maintained so that it can be retrieved under the name of an American if it relates to, for example, national defense or to national security of the Nation.

Now, I think there should be a general prohibition on indexing under the names of American citizens with some exceptions that have to do with an ongoing investigation of whether a person is an agent of a foreign power or evidence of criminal activity, but that there should not be a general authorization to index information under the name of an American citizen simply because the American citizen talked to a foreign embassy about national defense or national security of the United States.

The second issue has to do with the possible use of information from such electronic surveillance in a court in a criminal proceeding. There I think the bill violates what I understand to be the settled constitutional principle, and that is that if a criminal defendant would be entitled to information which the Government declines to release on national security grounds, the Government faces the choice of making the information available or dropping the prosecution. National security cannot be the basis for withholding information from a criminal defendant that he or she would otherwise be entitled.

The bill violates that principle in two places. One, it suggests that even if the Government intends to use the fruits of a national security electronic surveillance in a criminal case, it need not turn over the authorization to the defendant unless the court finds that that is necessary for the purpose of making a finding about legality. I think the normal procedure, the one that has to be followed here as well, is that if the Government wants to use the fruits of one of these wiretaps in a criminal prosecution, it must turn over the authorization to the defendant so that he or she can contest the legality of the surveillance or

whether the surveillance was conducted pursuant to the court order, that the judge simply cannot do that alone without depriving the defendant of due process.

Second, the provisions of the bill seem to me to clearly violate the Supreme Court's interpretation of the Constitution in the *Alderman* decision. *Alderman* says very clearly that if a judge finds that the surveillance is illegal, the fruits of the surveillance must be turned over to the defendant so that the defendant can prove that the evidence presented in the case was tainted by the illegal electronic surveillance.

The bill provides simply that if a judge finds that the surveillance is illegal, he should suppresss any evidence that the Government intends to introduce based on that illegal surveillance, and I think that that limitation is a violation of *Alderman* and a violation of the constitutional principle.

The CHAIRMAN. Well, now, maybe this doesn't go as far as you would like it to go. It does say information obtained or evidence derived from unlawful surveillance.

Mr. HALPERIN. Suppress the information, but *Alderman* says that you are entitled to the record in order to prove that the evidence that the Government in fact is introducing derived from electronic surveillance. The Court in *Alderman* pointed out that that is not a decision that the judge can make because he does not know enough about the facts of the case to be able to tell whether the illegal surveillance provided the clues that led to the evidence that is actually introduced. Therefore, the Court said if there is an illegal surveillance, the person who was illegally surveilled is entitled to the logs to prove that the evidence introduced is tainted.

The CHAIRMAN. Of course, what we say here, Mr. Halperin, is "in accordance with the requirements of law, suppress information obtained or evidence derived from an illegal or unlawful electronic surveillance."

Mr. HALPERIN. Yes, but the provision says—the provision, notwithstanding any other law, if the Government asserts that it would harm national security, these procedures should be used.

Now, it may simply be a drafting problem, but I think it has got to say that if the court determines that the electronic surveillance of the aggrieved person was not lawful or authorized to be conducted, the Court shall in accordance with the requirements of law, suppress the evidence obtained, and provide the fruits of the surveillance to the defendant. That is the requirement of the Constitution as the Supreme Court has interpreted it.

The CHAIRMAN. Well, let us look at that to make certain that what we are saying here is what we are trying to accomplish. We are advised that one of the sensitive problems in this area is certain foreign embassies.

Mr. HALPERIN. Well, I understand that, and as I understand it, a foreign embassy tap would not be illegal, and the provision to turn over the logs only arises if the Court finds the surveillance is illegal. The Court can, under *Alderman*, make an *ex parte, in camera* determination that the surveillance is legal. If it makes that determination and the Government chooses not to introduce the logs themselves into evidence, then there is no requirement to turn the information over.

The CHAIRMAN. Let's see if we can't clarify this. What you are in essence saying is that requirements of law require more than just suppression, making available information so that you see whether other evidence is used as a result.

Mr. HALPERIN. Right, where there is a finding of illegality.

The CHAIRMAN. Let's see if we can be more specific on that.

Mr. SHATTUCK. A couple of other points, Mr. Chairman. We recognize that you did want our informed view on the bill, and I apologize if in some respects we are not covering all the territory that we might.

The CHAIRMAN. Well, we have your statement.

Mr. SHATTUCK. We wish to study the proposal that has been furnished to us this morning in some detail, but we do recognize it as a substantial step forward, and are pleased, of course, to be able to review it for you.

A couple of additional points that don't appear in the proposal this morning. One is the question of the review that the Court might make of the certification by the Attorney General that foreign intelligence information is in fact likely to be obtained through a particular wiretap.

We share the concerns that you expressed in the Judiciary Committee and last year as well, about the scope of review that the Court might conduct to determine that in fact foreign intelligence information is going to be obtained. Under this bill, the standard is limited to clearly erroneous, and we would suggest that it should be broadened so the Court can play a more significant role in determining whether or not the information that is at stake is in fact foreign intelligence information.

An additional point concerns the reporting obligations the bill would impose on the Attorney General, to this committee and to the Congress. In order to make sure that this scheme, if it is to be enacted, works properly, it is necessary for Congress to obtain more information about the operation of wiretaps conducted under the bill than they can now obtain under the bill as drafted. We suggest that authorization information—not logs, but authorizations of particular taps—be made available to Congress either on a request basis or on a routine basis, but certainly so the Congress can look more searchingly into the conduct of the scheme that would be set up by the bill.

And let me conclude by reiterating how important we feel the solution of the foreign visitor problem is. I know it has been discussed in your opening statement, and we want to be sure that foreign visitors, not simply foreign powers, businessmen, tourists, mothers-in-law, et cetera, are given substantial protection, considerably more than they now have under the bill, and I think the proposal for determining whether the country from which they are traveling is in fact a country that engages in the kinds of activities that the bill is intended to look into is one for the committee to explore.

Then the terrorism definition prohibition against the targeting is extremely important to us. And finally, the political activity, the interception of political information protected by the first amendment, is extremely important.

We will be reviewing all of this language in a more careful and detailed way than we have been able to this morning, but we do commend the committee and you, Mr. Chairman, for this effort to advance the legislation by moving toward a criminal standard.

Of course, the improvement that we see is by no means everything that we feel is necessary under the fourth amendment law, but we do want to recognize it as an advancement, and to commend you for going in that direction.

The CHAIRMAN. Thank you, gentlemen.

Are there questions from the committee?

Senator HUDDLESTON. Does the panel consider the definition of terrorism in the Executive order to be adequate?

Mr. BERMAN. Excuse me, sir?

Senator HUDDLESTON. Do you consider that a correct definition or adequate definition?

Mr. BERMAN. We think it is a more definite statement of what the intentions of this legislation are aimed at by really nailing it down to international terrorist activity. I don't think we are happy with all of the definition in the Executive order. We call attention to section 4-209(a). There is a part of the definition of section 4-209(b) which says "appears intended to endanger a protectee of the Secret Service or the Department of State." It is difficult to understand why that is terrorism. The gist of terrorism is it is violent activity which is intended to intimidate and influence a population in terms of its political social or economic goals, and therefore is an ambiguity in the definition, but we do commend to the committee the section that deals with trying to define international terrorism.

The CHAIRMAN. Well, if there are no further questions and no further comments, gentlemen, thank you very much. We will continue.

Mr. BERMAN. One final point. I hope that we can work toward clarifying the criminal standard on terrorism, which is the most troublesome of what has been discussed this morning, in terms of nailing it down to activities that parallel the other sections. The proposed language here seems to allow surveillance even if there is no activity whatsoever, I mean, just a suspicion on the part of an intelligence agency. That is too broad for the use of an intrusive technique such as wiretapping, and we have to remember that you have to view the use of these techniques in terms of different investigative jurisdictions that will be spelled out in the charter. The FBI or the CIA will not have their hands totally tied waiting for violence to occur even if they can't wiretap.

The CHAIRMAN. Well, I hope you will look at this new language that I addressed myself to a moment ago and get your counsel on that.

Thank you very much, gentlemen.

Mr. SHATTUCK. Thank you very much.

Mr. BERMAN. Thank you.

The CHAIRMAN. Our next panel this morning is Mr. Steven Rosenfeld of the New York Bar Association and Mr. David Watters of the American Privacy Foundation.

Gentlemen, thank you for appearing. Why don't you go ahead and start.

TESTIMONY OF STEVEN B. ROSENFELD ON BEHALF OF THE COMMITTEE ON FEDERAL LEGISLATION, THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK

Mr. ROSENFELD. Thank you, Mr. Chairman. The train just got me here about 11 o'clock so I did not hear most of what went on this morning. I have not had a chance to review your opening statement, but your staff did read the language to me on the telephone, and I think I can address myself at least provisionally to it.

I am pleased to be here today to represent the views of the Committee on Federal Legislation of the Association of the Bar of the City of New York concerning S. 1566.

Our Committee is charged with the responsibility of developing and presenting the views of the association on proposed federal legislation of a diverse nature. For the past several years our committee has maintained a keen interest in the areas of domestic and foreign intelligence and has produced several reports on this subject. Our full views on S. 1566 are set forth in a longer prepared statement which is dated January 24, and which has been previously made available to the committee staff, and which I respectfully request be made part of the record.

The CHAIRMAN. Without objection, so ordered.

[The prepared statement of Mr. Rosenfeld follows:]

PREPARED STATEMENT OF STEVEN B. ROSENFELD ON BEHALF OF THE COMMITTEE ON FEDERAL LEGISLATION, THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK

I am gratified to be here today to present the views of the Committee on Federal Legislation of The Association of the Bar of the City of New York concerning S. 1566, the Foreign Intelligence Surveillance Act.

As this Committee is undoubtedly aware, our Committee is charged with the responsibility of developing and presenting the views of The Association of the Bar of the City of New York on proposed federal legislation of a diverse nature. For the past several years, our Committee has maintained a keen interest in the areas of domestic and foreign intelligence. In addition to commenting on previous versions of the legislation currently under consideration, we released last year a major report on Legislative Control of the FBI (Federal Legislation Report, May 1, 1977) which touches upon many of the same questions raised by the present bill. A review of that report may provide further insight into our Committee's views on these issues. Finally, a formal Report on S. 1566, which will contain all of the comments which follow, will be forthcoming very soon.

To begin with, our Committee applauds the basic intention underlying S. 1566, which is, we believe, to minimize, not encourage, electronic surveillance and to safeguard individual expectations of privacy against unwarranted government intrusion. In 1976, we supported enactment, with modifications, of S. 3197 (Letter to Sponsors of S. 3197, July 1, 1976). Three years ago, the Association also recommended passage of Senator Nelson's Surveillance Practices and Procedures Act (S. 2820) in a full report prepared by our Committee and the Committee on Civil Rights (Federal Legislation Report No. 74–4, June 24, 1974). While we do not deny the need for an effective foreign intelligence-gathering capability, disclosures of the past two years make it apparent that the kind of legislation we have supported since 1974 is also needed to protect individuals, whether citizens or aliens, from intrusion upon their fundamental rights and liberties. The judicial warrant procedure established by S. 1556 is certainly a major step in that direction.

We do not agree wth the view that the bill legalizes more electronic surveillance than it inhibits. We are made uneasy, however, by recent indications[1] that

[1] See H. Schwartz, "Taps, Bugs and Fooling the People" (Field Foundation, 1977); T. Wicker, "In the Nation," *The New York Times*, July 13, 1977, p. 29 and July 15, 1977, p. A.23.

the warrant procedure established by the Omnibus Crime Control Act of 1968 for surveillance in domestic law-enforcement may not be working—that surveillance applications and requests for extensions of surveillance are simply being rubber-stamped. As the Supreme Court reaffirmed last June in *United States* v. *Chadwick*, —— U.S. ——, 45 U.S.L.W. 4797, 4799 (June 21, 1977), the judicial warrant is supposed to provide "the detached scrutiny of a neutral magistrate, which is a more reliable safeguard . . . than the harried judgment of a law enforcement officer." If we are not getting such "detached scrutiny," the fault lies with the judges who are evading the responsibilities placed upon them by the Constitution and the 1968 Act, not with the judicial warrant procedure itself. We think the remedy is in the careful selection of the judges who will hear warrant applications under the new law and in expanded congressional oversight provisions, not in abandoning the traditional concept of a judicial warrant as a safeguard to personal liberties. We remain convinced that an effective warrant procedure which makes surveillers stop, think and justify their intended actions, especially when coupled with the other procedural safeguards and sanctions contained in S. 1566, is far more likely to minimize invasions of privacy than relying on undefined concepts and haphazard judicial review.

Our Committee is thus in agreement with the purposes of S. 1566. Our 1974 Report reviewed the historical background and considered the constitutional questions presented by such legislation. Our conclusion in the 1974 Report, that legislation subjecting foreign intelligence surveillance to judicial warrant procedures does not unconstitutionally restrict presidential power, is consistent with the conclusion expressed by former Attorney General Levi in his March 1976 testimony before the Subcommittee on Criminal Laws and Procedures of the Senate Judiciary Committee.

We are gratified to note the elimination of Section 2528 of last year's bill, and the corresponding repeal of Section 2511(3) of Chapter 119, both of which purported to recognize an inherent constitutional power of the President to conduct surveillance activities. The Supreme Court in *United States* v. *United States District Court*, 407 U.S. 297 (1972) left open the question of whether there was any such inherent power with respect to foreign intelligence activities. The hearings and reports of the two Select Committees have made it clear that the FBI has always relied upon the alleged inherent constitutional power of the President to conduct intelligence activities for the reasons set forth in 18 U.S.C. § 2511(3) (*i.e.*, to obtain information "deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities") as the principal, if not sole, source of its power to engage in the very activities which new legislation should seek to eliminate. There is no reason why Congress should expressly recognize any such power in the text of new legislation.

A. THE COMMITTEE'S MAJOR CONCERNS

Notwithstanding our support for the basic goals embodied in S. 1566, the members of our Committee are troubled by five major features of the bill:

1. The adoption of a "non-criminal" standard for permitting electronic surveillance against individuals;

2. The restriction of certain basic protections of individual privacy only to citizens and resident aliens, excluding all other persons;

3. The absence of any requirement to justify before a judge the asserted need for surveillance or the likelihood that foreign intelligence information will be obtained;

4. The possibility that the bill may be read to sanction the use of evidence obtained by foreign intelligence surveillance in criminal and other proceedings based only upon *ex parte* determinations, without any adversary hearing of any kind; and

5. The definition of "electronic surveillance" in § 2521(b)(6) appears to be limited in such a fashion as to permit both wholesale interception of international communications to and from the United States and unfettered retention and dissemination of the information so obtained, so long as the communications of particular United States persons are not targeted.

Before discussing the points mentioned above, I might first express our concern over the bill's failure to state in clear, recognizable and unambiguous terms that the procedures set forth therein constitute the sole lawful means of obtaining foreign intelligence information through electronic surveillance,

and that any other means are prohibited. We note with satisfaction the Judiciary Committee's statement (S. Rep. No. 95–604, November 15, 1977, p. 6) that this legislation, when combined with title 18, chapter 119, "constitutes the exclusive means by which electronic surveillance . . . and the interception of domestic wire and oral communications may be conducted." It is that exclusivity which, in the last analysis, wins our support. But we are concerned about the location of the exclusivity provision, which appears only deep after the semicolon in the second clause of § 4(c)(3)(f) of the bill. Subsection 4(c) is basically concerned with various conforming amendments to provisions of the 1968 Act which, as a group, carve out various exceptions to the mandatory warrant procedures. We would prefer to see the expression of this bill's basic intention that there shall be no surveillance except in accordance with the procedures mandated by law also appear in § 2522, which authorizes application for warrants under the new procedures. In our view, that is the proper place to make it clear that such procedures are the exclusive means of electronic surveillance and that any surveillance which is not in accordance with such procedures is prohibited.

I turn now to our Committee's major concerns about the standards of surveillance and the required showing to obtain a warrant under the bill. As the bill is structured, the definition section is crucial to its scope, particularly the definitions of "foreign power," "agent of a foreign power," and the term "clandestine intelligence activities." In their present form, these definitions are in some respects at odds with the approach the Association of the Bar has consistently adopted. As expressed in our 1974 Report (p. 14):

> This Association has been on record since the early 1960's in favor of the proposition that individual privacy must be protected by establishing a narrowly and clearly defined area of permissible electronic surveillance. Running through our successive reports there appears as well to have been a continuing minority view that the prohibition against electronic surveillance should be absolute.

With this approach in mind, in our comments on the 1976 bill we questioned the vague definition of the phrase "agent of a foreign power—particularly the absence of any requirement that the individual to be surveilled have knowledge of the involvement of a foreign power and that such involvement be apparent and direct. We are pleased to note that S. 1566 refines the definition of that term to require "knowing" action undertaken "for or on behalf of" a foreign power. The Committee nevertheless remains troubled that, under S. 1566, individuals may still be subject to electronic surveillance without any showing that they are engaged in, or likely to be engaged in, criminal activity. Even with respect to United States citizens and resident aliens, § 2521(b)(2)(B)(iii) would permit electronic surveillance based upon alleged conduct—clandestine collection of transmission of information to a foreign intelligence service—which is not clearly criminal. Our Committee has always been wary of making any exceptions to a strictly criminal standard where individual privacy is at stake and we are not persuaded of the need to depart from that position in this bill.

We are likewise disturbed that the bill's full protection of individual privacy is extended only to United States citizens and resident aliens. The Fourth and Fifth Amendments protect all "persons" and do not distinguish between United States citizens or resident aliens on the one hand, and other individuals within our borders on the other.[2] We hope that Congress will act to insure that the rights and liberties enunciated in the Constitution are equally available to all individuals who come within our borders. Under the present definition of "agent of a foreign power," thousands of innocent aliens—such as employees of foreign national airlines and other businesses owned or controlled by foreign governments, as well as tourists who simply happen to be employees of foreign governments or entities controlled by foreign governments, would be subject to electronic surveillance, without any further showing, the moment they arrive in the United States.

We would thus strongly urge adoption of a standard which treats all individuals alike, and requires a probable cause showing of criminal clandestine intelligence activity to justify a warrant. Recognizing, however, that the enactment of this bill must reflect a balancing of interests between constitutionally protected liberties and the responsibility of the Executive branch to protect

---

[2] *United States* v. *Toscanino*, 500 F. 2d 267, 280 (2d Cir. 1974); *Au Yi Lau* v. *United States Imm. & Nat. Serv.*, 445 F. 2d 217, 223 (D.C. Cir. 1971), *cert. denied*, 404 U.S. 864 (1971).

national security, the Association would support enactment of S. 1566 even with the present definitions and the "non-criminal" standard. However, illustrative of the strength of the Association's preference for a strict criminal standard, I should note here that the Civil Rights Committee of the Association would not support this legislation with the "non-criminal" standard and would prefer to see no legislation rather than enactment of this bill. That Committee's views are set forth in a separate letter to the Committee.

We would also urge the following changes to minimize the threat to individual privacy inherent in the present definitions:

(a) We noted in our comments on the 1976 bill that the phrase "clandestine intelligence activities" lacked any clear meaning, especially when used together with "sabotage" and "terrorism" which carry definite connotations of clear and present danger to domestic well-being. We are pleased that both "sabotage" and "terrorism" have been expressly defined in S. 1566, but are disappointed to find no comparable attempt to define the much vaguer term "clandestine intelligence activities." A satisfactory definition, which embodied the concept of "significant threat to the national security," appeared in the Judiciary Committee's report on S. 3197 (S. Rep. No. 94-1035, at 24). We believe that this phrase, like the other operative terms in the bill, should be given an express definition in the legislation itself, not relegated to a committee report.

(b) While we similarly approve the attempt to make more explicit the definition of the term "foreign power," we are troubled by the expanded scope of that term, especially since the bill now places practically no burden of proof on the applicant, and grants practically no power of review, where the target of the surveillance is a "foreign power" as defined. While we can understand that there may be some need for a different standard where the target is in fact a foreign government entity (or the equivalent), as noted in our 1974 Report (p. 12), the Fourth Amendment does not lose its force simply because foreign intelligence gathering may be involved. Wiretaps and bugs on foreign embassies, for example, must necessarily extend to those individuals who communicate with the embassies. We wonder if the national interest would really be threatened by requiring our Government to justify in court at least *some* need for surveillance of foreign embassies each time such surveillance is sought.

Whatever may be said concerning surveillance of foreign governments, we are not convinced that a need has been shown for treating in the same category all entities "directed and controlled" by foreign governments—for example purely business corporations, such as airlines, or United States corporations engaged solely in commercial and trade activities on behalf of foreign governments—without requiring the applicant to show probable cause to believe that the target is in fact engaged in intelligence activities. Absent such evidence of need, we would favor treating such corporations in the same way as individual "agents of a foreign power."

(c) As we urged last year, we still believe that the judge who passes on an application should be made aware of the sources of the applicant's alleged knowledge as to the facts required to be set forth in the application and the basis for believing such sources to be reliable. While we do not urge the disclosure of the identity of confidential informants, we do believe that information showing the reliability of sources will often be essential for the court to make any meaningful findings as required by the Act. See, e.g., *Spinelli* v. *United States*, 393 U.S. 410 (1969). At the very least, information as to sources of the applicant's knowledge should be within the scope of the "other information" which the judge may require under § 2524(c).

(d) The probable cause finding required under § 2525(a)(3) should include a third element—a finding that there is probable cause to believe that the information sought to be obtained will in fact be "foreign intelligence information" as defined in the bill. Without that third element, the warrant procedure does not really protect against surveillance instituted under this Act, but which is really designed to obtain information totally unrelated to foreign intelligence purposes, when the applicant could not obtain a warrant under existing law. Thus, while it is certainly some improvement over last year's bill to permit the court—where the target is a "U.S. person"—to review the basis for the certification specified in § 2524(a)(7), we are not at all satisfied with the rigid standard of "not clearly erroneous"—especially since the finding can be based only on the facts set forth in the certification itself. If there is in fact a growing tendency for rubber-stamping such applications, we believe that the "not clearly erroneous" standard amounts, in effect, to no review at all. That standard may

be appropriate for appellate review of factual findings after an adversary trial on a full record, but we cannot conceive of any situation in which, based only upon the minimal amount of information which the applicant must place before the judge, and with no one to present an opposing view, the certification could ever be held "clearly erroneous."

What is really required is that, instead of simply filing a certification which can be disturbed only if found to be "clearly erroneous," the applicant should be required to show probable cause to believe that the information sought is likely to be "foreign intelligence information" and that such information cannot be obtained by other means.

Without these changes, we do not think the bill can completely "curb the practice by which the Executive branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it," as claimed in the Judiciary Committee's Report (S. Rep. No. 95–604, p. 8).

(e) As we urged last year, we think the bill would be strengthened by requiring the surveillance order to include an express finding that the procedures of the Act have been fully complied with. It is one thing to legislate a set of procedures and to enact civil and criminal sanctions for violating them, but there would be more protection if the judge in issuing the warrant were required at that point to satisfy himself that there had been no procedural violation.

Our fourth major concern has to do with the provisions of § 2526(c) which can be read to permit the elimination of any adversary hearing prior to the use of information, obtained by foreign intelligence surveillance, against an individual in a trial, hearing or other proceeding. Notice and an opportunity to be heard is the mainstay of our system of due process. This bill would appear to permit such a hearing to be dispensed with, and a completely *ex parte* determination made, solely upon the filing of a government affidavit asserting "that an adversary hearing would harm the national security or the foreign affairs of the United States." We find the provision to be abhorrent to basic concepts of due process and, believe that there is a substantial possibility that it is unconstitutional, at least with respect to criminal proceedings. If the Government truly believes that an adversary hearing would harm the country, its choice should be to forget about using the information, not to forget about due process.

We do not oppose the requirement that, in appropriate cases, the surveillance application, order and transcript of surveillance be reviewed initially *in camera* (although we prefer last year's language which permitted the judge to disclose portions thereof to the aggrieved person upon finding that disclosure "would substantially promote a more accurate determination of the legality of the surveillance," to the language of S. 1566 which would require a finding that such disclosure "is necessary for an accurate determination"). We would, therefore, favor retention of the *in camera* review, but strongly urge elimination of the language which can be read to avoid the holding of any adversary hearing prior to use of the information against an individual.

Our last major concern arises out of the limitations on the definition of "electronic surveillance." Although we do not profess to have the technical expertise to assess fully the impact of the definition in Section 2521(b)(6), it appears to us that the definition excludes from the bill's coverage routine interception, by the National Security Agency for example, of every telephone call from the United States to a foreign country, so long as a particular United States person is not targeted and the call is intercepted at a location outside the United States or at a point when it is not being sent by wire. Thus, since the exclusivity provision of Section 4(c)(3) is limited to "electronic surveillance" as so defined (plus interception of domestic wire communications under Title 119), the bill would not cover wholesale interception of all international telephone calls, either from a ship stationed in international waters or from a point in the United States if the interception occurs while the calls are being transmitted by microwave or by satellite. In such cases, not only would the interception not be covered by the bill's warrant procedure, but there would be no controls on retention, dissemination or use of any information so obtained, because the "minimization" provisions of the bill are also tied to the definition of "electronic surveillance." Our interpretation of this definition is confirmed by the Judiciary Committee's Report (S. Rep. No. 95–604 at pp. 33–35).

We can see no justification for permitting wholesale electronic surveillance against all of us at once when we strictly limit such surveillance against identified individuals and groups. Even if the technical capability has not yet been developed to intercept at a point outside the United States, record and analyze

all international telephone calls, such an eventuality seems to us to be disturbingly within the realm of possibility.

Even if wholesale interception of international calls is to be permitted, the bill should at least be amended to include additional safeguards against retention, use or dissemination of information obtained from such interception. To accommodate the needs of our intelligence agencies, the contents of any such communications which constitute foreign intelligence information should be disseminated or used solely for foreign intelligence purposes. But so long as the information has not been obtained pursuant to the judicial warrant provisions of titles 119 or 120 and the person sending, or the intended recipient of, such communication has a reasonable expectation of privacy, dissemination even for criminal law enforcement purposes should be prohibited. Adoption of such a restriction would at least ensure that the law enforcement apparatus of the country must continue to abide by the Fourth Amendment in using information obtained by wholesale, intrusive electronic surveillance methods.

B. ADDITIONAL COMMENTS AND SUGGESTIONS

We have the following additional comments and suggestions for improvement of the bill, many of which were set forth in our letter of July 1, 1976 addressed to S. 3197. We present these comments section by section.

1. *Section 2521.* Most of our comments on the definition section were included in our discussion of the Committee's major concerns. We add only the following:

(a) We applaud the attempt to make the definition of "foreign intelligence information" more explicit. Nevertheless, for the reasons stated by former Senator Tunney in presenting his dissenting views in 1976 (S. Rep. No. 94-1035, 94th Cong., 2d Sess. at 135-36), we would favor insertion into § 2521(b)(5)(A) of the phrase "with respect to a foreign power or foreign territory," which now appears only in subsection (B) of that definition.

(b) With the major reservation previously expressed, we were pleased to see the expansion, from the version appearing in S. 3197 of the definition of "electronic surveillance" (§ 2521(b)(6)) to include interception of wire and radio communications sent by or intended to be received by United States persons within the United States. But we also share Senator Bayh's view that this definition does not go far enough and ought also to cover interception by their own government of communications sent or received by United States persons while outside the United States.

2. *Section 2523.* Especially in view of recent indications that some judges may not be fulfilling their responsibilities under the 1968 Act, we believe that several changes should be made to strengthen the section with respect to designation of judges and their conduct under this bill:

(a) As we noted in 1976, we believe it would be wise to limit the service of such judges to finite terms, such as three years, in order to permit fresh approaches and fresh insights to be brought to bear on these problems.

(b) Also in order to permit the application of diversified approaches, we favor a requirement that the number of designated district judges be increased to ten, to be selected from each of the ten judicial circuits by the Chief Judge of each circuit. Selection by the Chief Judge of each circuit, rather than the Chief Justice of the United States, avoids placing the Chief Justice of the United States in the position of having to pass upon petitions for certiorari from the determinations of the very judges he has personally selected. Likewise, we favor a requirement (which is probably implicit anyway) that the three judges designated to serve on the special court of review not include any of the judges designated to hear applications and grant orders.

(c) The prohibition against submitting the same application to different judges for the same electronic surveillance once denied is a sound addition to the bill. However, the provision for a special court of review in effect constitutes an opportunity to "try again," since § 2523(b) does not give the special court any standard for review, other than to determine whether "the application was properly denied." We would not favor *de novo* review by the special court and thus urge that the bill set forth the requirement for a reversal of denial of an application, such as a holding that the denial was an "abuse of discretion."

(d) As we said in 1976, we also favor a requirement that the written statements of the district judges and of the special court of review, explaining the reasons for denials of warrants, be published, with suitable redaction to prevent

the disclosure of the identity of proposed targets of surveillance and other confidential details. We would be content to leave to the discretion of each court precisely what material should be omitted from the published statements, but we think that publication of the statements, and the development of a body of law under the Act, would substantially further its purpose.

3. *Section 2524.* Most of our comments concerning the warrant procedure itself are set forth above in the statement of our major concerns. We have the following additional comments:

(a) Even if there is some need for a less rigid standard when the target of surveillance is a foreign power, as defined, rather than an individual, we are not convinced of the need for excepting foreign power surveillance from each of the requirements from which it is now excepted. For example, we do not see why the applicant should not be required to set forth the basis for his belief that the information sought is foreign intelligence information or that normal investigative techniques are insufficient. We would recommend further consideration of the need for each of these distinctions.

(b) Section 2524(c) of the 1976 bill provided that the judge may require the applicant to furnish "such other information or evidence as may be necessary to make the determinations required by § 2525". S. 1566 eliminates the phrase "or evidence". We are concerned that this change may be read as an indication of intent to prohibit the judge from requiring the "additional information" to be presented in the form of sworn testimony or other competent evidence. We understand that there was no such intention (and we would seriously question any such intent). We would, therefore, urge that the phrase "or evidence" be restored to § 2524(c) or at least that the legislative history make clear that there was no intent to preclude the judge from taking evidence.

4. *Section 2525.* We have the following additional comments on this section of the bill:

(a) While, as noted above, we question the extremely narrow standards of reviewability of the certification set forth in § 2525(a)(5), even if that standard is to be retained, we do not understand the reasoning behind limiting the review to cases where the target is a "United States person". In all other similar sections of the bill, where a distinction is made in the statutory standards, the distinction is between "foreign power" and "agent of a foreign power". Because, as noted, we think that non-United States persons have rights and liberties worthy of protection, we would at least urge that the judicial review afforded in § 2525(a)(5) be extended to all applications where the target is not a "foreign power" as defined.

(b) We appreciate that there may be rare emergency situations in which the procedures set forth in § 2525(d) will be required. Because we share with many of the sponsors of the bill the assumption that such situations will be rare, we would urge that the bill require the Attorney General to report to this Committee (or some other suitable congressional oversight committee) each time the emergency powers are used, at the same time as an application is made for the after-the-fact warrant provided for in the bill. We believe that such a prompt reporting requirement will go a long way to insuring that the emergency power is not abused.

5. *Section 2526.* We have the following additional suggestions concerning the section on use of intelligence information:

(a) In its present form, § 2526(a) purports to limit the use of information obtained by foreign intelligence surveillance to "the purposes set forth in section 2521(b)(8)" or for criminal law enforcement. But § 2521(b)(3) contains only the bill's definition of "minimization procedures" and does not set forth any specific descriptions of the manner in which information may be used, much less any restrictions governing such use. Misuse of intelligence information has been an abuse at least as serious and far reaching as those involved in the gathering of such information. Legislation which regulates the intelligence-gathering process, but is practically silent on the permissible uses of intelligence, accomplishes only half the job. Regulating the use of intelligence information is neither impractical nor without precedent. Section 552(b) of the Privacy Act of 1974 (5 U.S.C. § 552a (b)), governing permissible uses of personal data in agency files, provides a model of such an effort which could be adapted with appropriate deference to the sensitive nature of foreign intelligence information.

(b) We are also concerned about the new language in § 2526(a) which would permit the use of information acquired from electronic surveillance for enforcement of the criminal law only "if its use outweighs the possible harm to the na-

tional security." The bill does not specify who is to make the judgment between the interests of law enforcement and possible competing interests of "national security." If that judgment is left to those who conducted the surveillance, the statute might have the effect of preventing the use of information acquired from such surveillance as evidence to prosecute violations of the Act itself. At the very least, we would favor an amendment to provide that such a determination may be made only by the Attorney General.

(c) We support the concept of "minimization procedures" as set forth in the bill, as one method of insuring the least possible intrusion upon individual privacy and liberties. We do, however, believe that the provisions with respect to minimization in S. 1566 do not go far enough. Specifically, we recommend the following:

(i) We note with approval the Judiciary Committee's amendment which makes it clear that the required notice of intention and judicial review prior to use or disclosure of intelligence information applies to state and local proceedings, as well as to federal courts and agencies. However, while it permits the disclosure of intelligence information to state and local law enforcement authorities (§ 2526(b)), S. 1566 still does not require such state and local authorities to observe the notice of intention procedure which § 2526(c) would place upon federal authorities. As we understand the bill, "the Government" as used in § 2526(c) refers only to the federal government, so that only federal agencies would be required to notify a court of intention to use or disclose the information, and obtain that court's advance determination of the legality of the surveillance. State and local authorities would only be required to obtain advance authorization of the Attorney General under § 2526(b), but no advance judicial determination. We can see no reason for such a distinction and we note that the provisions of Chapter 119 (particularly §§ 2515 and 2518(10) are not so limited. We would thus urge that § 2526(c) be made applicable to use or disclosure of intelligence information by state and local, as well as federal, authorities.

(ii) While we can anticipate the arguments in favor of permanent retention of information accidentally acquired which is neither "foreign intelligence information" nor evidence of a crime, we believe that, in the long run, there is no justification for preserving such information in government files where it can only be misused and put to no legitimate use. (See this Committee's Report on the Privacy Act of 1974, Federal Legislation Report No. 74–9, November 15, 1974.) Accordingly, we would propose that the bill include a requirement that, within a specified time after the termination of a surveillance in cases where such extraneous information is obtained, notice of that fact be given to the target of the surveillance (at least where the target is not a "foreign power") and such person be given the right to demand destruction of all such non-foreign intelligence information. To guard against dangerous or premature disclosure of the existence of ongoing investigations, this section could contain the same procedures for judicial postponement of the notice requirement as now appear in § 2526(f). An even broader notice requirement, together with similar provisions for judicial postponement, was included in the 1974 Nelson bill, and was supported by our 1974 Report. We again urge the adoption, as part of the required minimization procedures, of the notice requirement suggested above.

(iii) We are concerned that § 2526(b), which provides that minimization procedures shall not be deemed to preclude retention and disclosure of information incidentally acquired which is evidence of a crime, might permit law enforcement agencies to conduct illegal domestic surveillance under the guise of foreign intelligence surveillance, where they cannot meet a "probable cause" standard to obtain warrants for surveillance. We thus believe that the bill should contain an additional proviso that information or evidence incidentally obtained in the course of foreign intelligence surveillance, while it may be disclosed to the appropriate domestic law enforcement agencies, would remain subject to all of the established statutory and Fourth and Fifth Amendment protections and restrictions upon admission into evidence or other use in the criminal law enforcement process. The second sentence of § 2526(a) accomplishes this result only in part, since many of the protections we have in mind might not be properly characterized as "privileges" or as pertaining to "privileged information". We believe the full protection noted above is what is really required.

(d) Just as we do not approve a distinction between "United States persons" and other individuals with respect to the availability of judicial review of the certification under § 2525(a)(5), we do not approve the same distinction in § 2526(a). Although the sentence added to the end of § 2526(a) by the Judiciary Committee helps somewhat that section would still permit information acquired from electronic surveillance concerning persons who are not citizens or resident aliens to be used for undefined purposes at the discretion of the acquiring officials, with the only restriction being that such purposes be "lawful". As we have said before, the protections of the Fourth and Fifth Amendments apply to all persons, not only citizens and resident aliens, and we can see no reason to give federal officials undefined latitude in the use against individuals of information obtained from electronic surveillance. If there are "lawful purposes"—such as deportation proceedings—which apply only to foreigners, they should be expressly stated. But perpetuation of a distinction with respect to use of intelligence information between "U.S. persons" and all other individuals is, in our view, unjustified and may create constitutional infirmities.

(e) As we said in our comments in 1976, we think that the court's determination under § 2526(e) should include a specific finding that the procedures of this Act were complied with when the surveillance was undertaken.

(f) For the reasons stated in our 1974 Report we believe the notice requirement of § 2526(f) with respect to emergency surveillance which is subsequently not approved by the court, is an essential protection without which we would question the emergency power. We think, therefore, that the court should retain absolute discretion over any applications for dispensing with the required notice. Accordingly, we would urge that the verb "shall" in the last sentence of § 2526(f) be changed to "may."

6. *Section 2527.* We think that the Attorney General's annual report to Congress is an essential feature of the bill, providing the basis for a continuing oversight to insure that the statutory procedures are working as intended. We were thus dismayed to see that S. 1566 contemplates an even briefer, less meaningful, annual report than would have been required by S. 3197. We urge restoration of the portions of the required report which appeared in S. 3197—such as listing the number of surveillances terminated and the number currently in effect, and would also suggest inclusion of the following additional information:

(a) A summary of the reasons given during the year by the designated judges for denial of applications for surveillance. (This would be especially valuable in the event our suggestion that such statements by the judges be published is not adopted.)

(b) A statement of the total number of uses of the emergency power of § 2525(d) and the number of times subsequent court approval was not obtained.

(c) As to each of the surveillances terminated during the year, a statement of the time each remained in effect.

(d) A description of all pending civil and criminal proceedings for alleged violations of the Act and the position taken by the Justice Department with respect to each.

7. *Civil and Criminal Sanctions.* We support the inclusion of criminal sanctions for willful violations of the statutory procedures and civil remedies for damage caused by surveillance not undertaken in compliance with the statute. We cannot emphasize too strongly that a bill of this sort without criminal and civil sanctions is not a meaningful response to the abuses recently brought to light. We note especially that § 4(a) of the bill has been amended, as we urged in 1976, to make the scope of the crime enunciated in 18 U.S.C. § 2511 co-extensive with the scope of the new bill's definition of "electronic surveillance." However, the two specific criticisms of the civil remedy which we enunciated in 1976, still apply:

(a) We recognize that the civil remedy is keyed to the existing remedy created under the 1968 Act (18 U.S.C. § 2520). But we think the opportunity should be taken to make the civil damage provisions of § 2520 more meaningful. In today's economy, and considering the kinds of serious intrusions upon personnel privacy which have been disclosed by the Senate and House Select Committees, a damage award limited to $1,000 is neither meaningful compensation nor sufficient inducement for individuals to undertake federal court litigation to vindicate their rights. We believe that plaintiffs should be permitted to prove actual damages in an amount equal to the actual injuries they have suffered and that the formula of $100 per day or $1,000 per violation should be a minimum rather than a ceiling. While we approve of the provision for puni-

tive damages in egregious cases, the natural reluctance of judges to impose punitive damages makes that provision no substitute for actual compensatory damages in cases where unauthorized surveillance has, as sometimes happens, ruined an individual's social life, seriously interfered with his livelihood or caused provable damage to his reputation or his emotional stability.

(b) Even more important, the denial of standing to commence civil damage actions to anyone meeting the definition of an "agent of a foreign power" in effect limits the civil damage remedy to violations which resulted in surveillance of a person as to whom the Act does not permit surveillance. All other violations of the statutory procedures—such as filing false applications, misuse of the emergency powers, or even failure to obtain a warrant at all—would be immune from the civil sanction so long as the injured party is someone who could have been subject to surveillance if the Act was complied with. Thus, innocent individuals, such as non-resident aliens working in foreign embassies or U.N. missions, could be made targets of surveillance in violation of the statutory mandates or victims of unauthorized disclosure of intelligence information, and could suffer damage thereby, and be powerless to seek redress. Where such violations and resulting damage can be proven, we see no reason to deny standing to maintain an action.

We note in passing that this amendment preventing an "agent of a foreign power" from seeking civil remedies is so broadly drawn that a U.S. corporation which is owned by a foreign government would be denied monetary recovery from a U.S. competitor which conducts industrial espionage against the hapless company in violation of the antiwiretapping provisions of chapter 119 of Title 18.

* * * * * * *

On behalf of the Federal Legislation Committee, I am deeply grateful to the Committee for permitting me to express these views. It should be obvious that there are numerous ways in which our Committee believes that the Foreign Intelligence Surveillance Act can and should be strengthened to maximize the protection of cherished rights and liberties. But as Chief Justice Burger wrote last June in the *Chadwick* case, requiring surveillers to obtain a judicial warrant goes a long way toward protect[ing] people from unreasonable government intrusions into their legitimate expectations of privacy." (45 U.S.L.W. at 4790.) Thus, we believe that S. 1566 represents an important step toward ending the kind of abuse of the intelligence process which only serves to discredit our nation, and it has our full support.

LETTER TO SENATOR DANIEL INOUYE FROM GEORGE M. HASEN, CHAIRMAN, COMMITTEE ON CIVIL RIGHTS

JANUARY 24, 1978.

HON. DANIEL K. INOUYE,
Chairman of the Senate Select Committee on Intelligence,
U.S. Senate, Washington, D.C.

DEAR SENATOR INOUYE: We understand that your Committee has received from the Committee on Federal Legislation of the Association of the Bar of the City of New York its critique of the provisions of the proposed Foreign Intelligence Surveillance Act of 1977 (S. 1566). Our Committee on Civil Rights associates itself, generally, with that critique, but we disagree with it in one important respect.

Both the Committee on Federal Legislation and the Committee on Civil Rights are concerned because the standards imposed by S. 1566 for obtaining a warrant to engage in electronic surveillance do not, in some instances, require a probable cause showing of criminal conduct. It is the considered judgment of the Committee on Civil Rights that a criminal standard is essential to the bill and, unlike the Committee on Federal Legislation, we believe that unless S. 1566 is amended to provide such a standard, it should not be enacted.

We think it is important to remember why this legislation is needed. Clearly it is not needed to empower government agencies to carry on electronic surveillance. Rather, the need is for legislation which will limit and control electronic surveillance and the consequent government intrusion into the private lives of American citizens. The findings of Congressional committees which over the last several years have investigated intelligence agency abuses have made this need abundantly clear. Based on such findings, the Church Committee specifically

concluded that no American should "be targeted for electronic surveillance except upon a judicial finding of probable criminal activity" and, further, that 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 Rights of Americans, Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, U.S. Senate, 94th Cong., 2nd Sess. (1976), at 325.)

Further the Supreme Court has warned of the danger to First Amendment rights inherent in national security surveillances:

"National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. '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.' *Marcus* v. *Search Warrant*, 367 U.S. 717, 724 (1961). History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent.' *United States* v. *United States District Court*, 407 U.S. 297, 313 (1971).

Notwithstanding these warnings, S. 1566 would permit the electronic surveillance of United States citizens and other persons for 90 days or more without any showing that they are engaged in, or likely to be engaged in, criminal activity. Section 2521(b)(2)(B)(iv) would go even further and would permit the electronic surveillance of individuals who "knowingly" aid and abet persons whose conduct may be entirely lawful.

Surely, the burden of justifying such a departure from basic Fourth Amendment principles—if indeed it can be justified—ought to be on the proponents of such provisions. And, surely, they ought to be able to specify precisely those lawful activities of American citizens which are so vital to the safety of the nation that the Government must be permitted to surreptitiously gather information about them and, worse, to do so by such an intrusive method as electronic surveillance. In our opinion, however, two Attorneys General have been unable to sustain that burden, and the few examples which have been offered of lawful activity requiring electronic surveillance are simply unconvincing. In our view, the necessity of a non-criminal standard has not been demonstrated, and it should, therefore, be rejected.

There is another and perhaps even more important reason why such a standard should not be accepted. If, in this first legislative attempt to control searches in national security matters, Congress authorizes the most intrusive and least precise of techniques—electronic surveillance—where no crime is involved, what justification will there be for barring in similar situations more specific methods such as surreptitious entry and mail openings? And if a non-criminal standard is necessary to protect the national security where the connection with a foreign power can be as tenuous as that provided in S. 1566, what arguments can be made against a similar standard in domestic situations where the perceived danger to national security may be just as great?

S. 1566 represents in some respects an advance over earlier proposals, but in our view, if a non-criminal standard is retained, enactment of this legislation will legitimize the very conduct it ought to prohibit and will constitute a serious blow to civil liberties.

If permitted by your procedures, it would be appreciated if this letter were made a part of the record of the hearings of your Committee on this bill.

Very truly yours,

GEORGE M. HASEN,
Chairman, Committee on Civil Rights.

Mr. ROSENFELD. This morning I will simply mention the major points.

To begin with, our committee applauds the basic intention underlying S. 1566, which is, we believe, to minimize, not encourage, electronic

surveillance, and to safeguard individual expectations of privacy against unwarranted government intrusion. While we do not deny the need for an effective foreign intelligence gathering capability, disclosures of the past 2 years make it apparent that the kind of legislation we have supported since 1974, when we issued a report on the Nelson bill, is needed to protect individuals, whether citizens or aliens, from intrusion upon their fundamental rights and liberties. The judicial warrant procedures established by S. 1566 is certainly a major step in that direction.

We do not agree with the view expressed by some that the bill legalize more electronic surveillance than it inhibits. We are made uneasy, however, by recent indications that the warrant procedure established by the Omnibus Crime Control and Safe Streets Act of 1968 for surveillance in domestic law enforcement may not be working, that is, that the surveillance applications and requests for extension of surveillance are simply being rubber stamped.

As the Supreme Court reaffirmed last June in *U.S. v. Chadwick*, a judicial warrant is supposed to provide "the detached scrutiny of a neutral magistrate, which is a more reliable safeguard than the harried judgment of a law enforcement officer" and we think the same applies to intelligence officers.

If we are not getting such detached scrutiny, the fault lies, we believe, with the judges who are evading the responsibilities placed upon them by the Constitution and the 1968 act and would be placed upon them by the pending bill, and not with the warrant procedure itself. We think the remedy is in strengthening the provisions of this legislation to insure careful selection of judges who will in fact carefully weigh and not rubberstamp applications, and expanded congressional oversight provisions, but not in abandoning the traditional concept of a judicial warrant as a safeguard to personal liberties. We remain convinced that an effective warrant procedure which makes surveillers stop, think and justify their intended actions, especially when coupled with the other procedural safeguards and sanctions contained in S. 1566, is far more likely to minimize invasions of privacy than relying on undefined concepts and haphazard judicial review.

So, notwithstanding, Mr. Chairman, our support for the basic goals embodied in S. 1566, the members of our committee are troubled by five major features of the bill as it has been reported by the Judiciary Committee.

Our major concerns are discussed at pages 5 through 16 of the longer prepared statement; and they are briefly as follows:

First, we have always been troubled by any adoption of a noncriminal standard for permitting electronic surveillance against individuals, and we continue to prefer strongly a criminal standard at least for U.S. persons which relates to any actual or impending criminal activity, and indeed, illustrative of the strength of feelings within the city bar association on this subject, I should note here that the Civil Rights Committee of the association would not support the legislation in its present form with the non-criminal standard, and would prefer to see no legislation at all. That committee's views have been set forth in a separate letter to the members of this committee which they have also asked be included in the record.

Second, we question the restrictions of certain of the basic protections of the bill only to citizens and resident aliens, excluding all other individuals. I am sure the committee is aware that the Fourth and Fifth amendments of the Constitution protect persons and do not distinguish between U.S. citizens and resident aliens on the one hand, and all other individuals on the other hand. Under the present definition of "agent of a foreign power" thousands of innocent aliens, and I heard the earlier panel referring to this, such as employees of foreign national airlines or other businesses owned or controlled by foreign governments, as well as simply visitors who happen to be employees of foreign governments or entities controlled by foreign governments, would be subject to electronic surveillance without any further showing.

Third, we strongly prefer to see a requirement that the applicant justify before a judge under the probable cause standard, not only that the target is a foreign power or an agent of a foreign power, but also the asserted need for surveillance and the likelihood that foreign intelligence information will be the result.

We are very troubled by the not clearly erroneous standard of review which appears in section 2525(a)(5), and which applies to begin with only to U.S. persons. We are troubled especially since the finding, by the terms of the statute, of not clearly erroneous, can be based only on the facts which are set forth in the certificate itself. If it is true that there is a growing tendency of federal judges to rubber-stamp warrant applications, we wonder whether the not clearly erroneous standard amounts to any review at all. That standard may be appropriate and in fact derives from the situation of appellate review of factual findings after an adversary trial on a full record, but we cannot conceive of any situation in which based only upon the minimal amount of information which the applicant must place before the judge, and with no one present to—no one to present an opposing view, the certification could ever be held on that basis to be clearly erroneous.

As long as the clearly erroneous standard stays in the bill, we wonder whether it is true to say, as the Judiciary Committee did in its report, that the bill will curb the practice by which the Executive branch may conduct electronic surveillance on its own unilateral determination that national security justifies it.

Fourth, we are concerned about section 2526(b), particularly the possibility that it may be read to deny any adversary hearing of any kind to a person against whom surveillance material might be used in a criminal proceeding.

We understand the need for *ex parte* determinations and the possibility that all of the material that would be available to a judge in the *ex parte* determination might not be made available to the accused in a criminal proceeding, but a bill that allows for the possibility of no adversary proceeding at all, we think, is abhorrent to basic concepts of due process and raises unnecessary constitutional questions.

Finally, the definition of electronic surveillance in section 2521(b)(6) appears to be limited in such a fashion as to permit wholesale intereceptions, for example, by the National Security Agency, of all international communications to and from the United States and unfettered retention and dissemination of information so obtained.

We acknowledge the statement in the Judiciary Committee's report, and I think I noted it also, Senator Bayh, in your statement this morning, that there is an intention to deal with this problem in separate legislation, but until that is done, we feel that this legislation should at least make it clear that any information so obtained by a non-targeted reception of communications not being transmitted by wire or at a point outside the United States, should at least be used only for foreign intelligence purposes and no other purposes, and that is not in the present bill.

In addition to these major concerns, our committee's prepared statement contains numerous additional recommendations for specific changes in the bill which I will be glad to comment on when time permits, but which I urge the committee and the staff to look at carefully. These relate to such essential points as additional provisions governing the appointment and functioning of the designated judges, which we think might prevent the rubber stamping of warrant applications; second, making more meaningful the content of the warrant applications, and making clear what kind of additional information the judge might require; third, changes in the minimization and prenotification procedures of section 2526; as mentioned by Mr. Shattuck earlier, expansion of the required content of the Attorney General's annual report to Congress; and finally, and I personally feel most strongly about this, with respect to the limitations on damage awards, and what we view as unfair limitations on standing to sue in civil actions under this legislation which we feel could really eliminate civil actions as an effective enforcement mechanism.

Despite, and notwithstanding all of our specific concerns and suggestions, Mr. Chairman, our committee basically supports this legislation. As Chief Justice Burger wrote last June in the *Chadwick* case, requiring surveillers to obtain a judicial warrant goes a long way toward "protecting people from unreasonable Government intrusions into their legitimate expectations of privacy."

We think that S. 1566 represents an important step toward that end and we support it.

Thank you, Mr. Chairman.

The CHAIRMAN. If we could, if you don't mind Mr. Watters, just let us direct questions to Mr. Rosenfeld because I think your testimony is coming from a little different direction.

Are you more comfortable, or do you suppose that the civil rights section of the bar would support the bill with the new language as far as the criminal standard is concerned?

Mr. ROSENFELD. Well, Mr. Chairman, insofar as the new bill, and the section that is specifically related to violations of the criminal laws of the United States, it certainly goes a long way toward meeting our committee's concerns, and I did discuss it with the chairman of the Civil Rights Committee who of course was only hearing it from me on the telephone and had not, especially in view of the weather in New York yesterday, had a chance to discuss it with his Committee, but it was his view that it sounded like a good step in the right direction. He wasn't prepared to go further than that at the time I discussed it with him, but certainly it does resolve the concern expressed by our committee that activities which are not clearly criminal could still be the subject of surveillance.

The CHAIRMAN. You mentioned the resident alien problem.

Are you relieved any with the new language which specifies that this person is a national of a foreign nation which engages in clandestine activities in the United States, and the circumstances of such person's presence in the United States makes it likely that such a person is or may be engaged in such activities in the United States?

Mr. ROSENFELD. Well, Mr. Chairman, this is the first time I am hearing that language. Is that in the language——

The CHAIRMAN. That is in the revision.

Mr. ROSENFELD. That sounds like it might solve the problem of the employee of the foreign business concern which happens to be controlled by a foreign government or of a casual visitor to the United States who happens to be the employee of a foreign government.

The CHAIRMAN. I think that probably solves the second problem; but that probably is not sufficient for the first one, if I recall your concern.

In certification, we are trying to deal with the need for more information, but the way I understand your concern is that you believe that the defendant under certain circumstances might not receive the information.

Mr. ROSENFELD. Are we talking now about the use of the material in a prosecution or other proceeding?

The CHAIRMAN. The judge ought to receive more information in making a determination.

Mr. ROSENFELD. We accept the need for *ex parte* communications. Our concern is that section 2526(c) can be read to permit the dispensing with any adversary hearing of the subject. I think the defendant should always be given his day in court, even if he has to go on the basis of not seeing the warrant application and the other material on the basis of which the warrant was issued, but to say that the material should be used against him without any adversary proceeding I think offends due process and I don't see the need for it. I can't conceive of any situation in which the Government should be permitted to say that an adversary proceeding of any kind is so contrary to the national security that it should be dispensed with. I think if it gets to that point that is when the Government should make its election to drop the prosecution.

The CHAIRMAN. That is a question on how we best handle that.

Gentleman, do you have any questions?

Senator HUDDLESTON. No thank you.

The CHAIRMAN. Senator Case.

Senator CASE. You are talking about the use against a defendant in a trial, hearing or other proceeding. You are not talking about information that may enable police to circumvent action that may be taken.

Mr. ROSENFELD. No; I was just referring to section 2526(e).

Senator CASE. It's a little hard to say. You would just be using information in court, in an adversary proceeding, a criminal proceeding?

Mr. ROSENFELD. Yes.

Mr. Chairman, if I have 1 minute, I would like to go maybe a little bit more fully into our concerns about the civil damage action provision.

As presently drafted, the legislation limits standing to sue for any violations of the act to those who are not foreign powers or agents of foreign powers. This in effect means that the only time an individual would have standing to bring a civil damage action is when he is subject to surveillance, but is an individual who could not have been targeted for surveillance in the first place.

If he is an individual who could have been targeted for surveillance, but any one of the other requirements of the act was dispensed with or ignored, including the minimization procedures, which are the procedures that are precisely designed to prevent damage to the individual, he would not have standing to sue.

In fact, as presently drafted, the act would not give anyone standing to sue where the whole procedure of the act was just ignored and surveillance was conducted without a warrant at all.

We don't see any need for so drastically limiting the standing to sue, especially as the phrase "agent of a foreign power" has evolved over the various provisions of this act. We can conceive of many instances in which an individual person who is an agent of a foreign power would have a legitimate grievance, would have probable damages and ought not to be deprived of the chance to redress the grievance in a court proceeding.

The CHAIRMAN. Senator Lugar?

Senator LUGAR. Yes, Mr. Chairman, I would like to ask Mr. Rosenfeld, he mentioned the Committee on Civil Rights of the Bar Association of New York City, and I reviewed their letter as you mentioned. Clearly they come to a conclusion on the first page, and this is reiterated, that unless S. 1566 is amended to provide such a standard, including probable cause of criminal conduct, they feel we ought not to adopt this legislation at all.

Now, in your concluding statement, of course, you mentioned their letter and your own concerns and that of the bar generally in New York.

To what extent have any of the amendments that have been proposed or even amendments suggested by the chairman today alleviated either your concern or what you understand to be the concern of the Committee on Civil Rights? Is it possible that their viewpoint which was very severe, certainly on January 24, has softened or is likely to, given this dialogue.

Mr. ROSENFELD. Well, as I said to Senator Bayh, I think our committee's concerns would be substantially alleviated by the new language which was proposed in Senator Bayh's opening statement because it does in each of its sections relate in some measure to violations of criminal law. I did discuss it briefly with the chairman of the Civil Rights Committee yesterday. He didn't have the language in front of him, of course, and was unable because of the weather conditions yesterday to discuss it with the members of his committee, but he did authorize me to say that it looked like a big step in the right direction, that they would study it and provide their views to the Committee in a separate letter.

Senator LUGAR. This is what I wanted to ask, that in view of what is occurring and things that may occur today in this hearing, would it be possible that the Committee on Civil Rights, or for that matter, the

entire association, to write to the committee again for the benefit of the record?

Mr. ROSENFELD. Well, I am hopeful that this change might completely eliminate the intramural difference of opinion that did crop up over this one issue.

Senator LUGAR. Thank you.

The CHAIRMAN. Does the Civil Rights Committee think we need legislation in this area, or are they satisfied with the way things are right now?

Mr. ROSENFELD. No; I think they believe we do need legislation in this area. The 1974 report on the Nelson bill was a report of the two committees, and it did set forth the opinion that there should be only a criminal standard.

As I remember the Nelson bill, it did have a criminal standard, so there was no occasion for the two committees to part company. Of course that was also 1974. A lot has happened since then.

But I definitely think I can represent that they think there is a need for legislation in this area.

The CHAIRMAN. As I said before you arrived, we spent a great deal of time trying to resolve the criminal standard problem and none of us were happy with the lack of it. You and the civil rights section have performed such a worthwhile service continually to warn us about the importance of being constantly aware of violations in this area, I hope you might convey to them and to those who don't already understand it, the great difficulty of getting any legislation in this area, and that it involves a great deal of give and take to get as far as we are right now.

Mr. ROSENFELD. Mr. Chairman. I think that was the major consideration which in the final analysis won our committee's support for this legislation.

The CHAIRMAN. Well, I appreciate that, plus I appreciate the constructive comments you have made.

All right, Mr. Watters, thank you for your patience.

[The prepared statement of Mr. Watters follows:]

PREPARED STATEMENT OF DAVID L. WATTERS*

"J'aimerais mieux diner avec le bourreau qu'avec le Directeur général des Postes." Quesnay.

MICROWAVE EAVESDROPPING

An appropriate title for the few remarks I have today is Microwave Eavesdropping.

To the enginering community, the title perhaps would be "Broadband Interception Practices and the Interception of Non-Oral Communication."

A Constitutional lawyer might call it, "Considerations of Warrantless Instantaneous Electronic 'Search' of Private Communications Without 'Seizure' ".

This is an issue that has not received significant public airing before the committee; one which may set a terrifying constitutional precedent if not reasonably dealt with in S. 1566.

*David Watters is a telecommunication 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 AT&T. He is a native of Georgia.

INTRODUCTION

In his presentation on this subject last July, Senator Moynihan told us that, "For some years now, we have been concerned with the manner in which sophisticated electronic technology threatens the traditional right to privacy guaranteed Americans by the Constitution of the United States." He said that, "The record is clear on this point: intelligence agencies of this [our own] government have, in the past, acted improperly, and individual citizens have suffered thereby."[1]

The result of Mr. Moynihan's effort was a bill cited as the "Foreign Surveillance Prevention Act of 1977" presented as a means to expel foreign agents of the Soviet Union and other world powers whenever there is reason to believe that such persons are engaging in electronic surveillance within the United States.

The real thrust of Mr. Moynihan's assertions, however, is that both foreign and American intelligence agencies are engaging in an unprecedented electronic warfare within our national telephone network, primarily the microwave system, a warfare involving billions of dollars, and at a scale greater than that during the height of the Viet Nam war.

The irony of this warfare is that it is of questionable cost effective value to either of the adversaries, and that the real losers in the battle are the innocent Americans whose privacy is being invaded.[2]

Senator Moynihan said that, "yet a curious—even eerie—unwillingness exists to confront not merely the dimensions of the problem, but also to imagine that we in the United States can do anything about this!"

My purpose is to show that present laws are not providing the protection the American people need, under the Constitution; and that the proposed statute, S. 1566, is inadequate, and will continue to be inadequate even if all the suggestions of the civil libertarians concerning the strict definitions of "foreign agent" and "criminal standard" are maintained.

I hope to offer some constructive language to be used in S. 1566, and to suggest some reasons why this language should be adopted.

Incidentally, as a southern conservative, I stand beside the civil libertarians in the line drive against the non-criminal standard for electronic eavesdropping. The thrust of my presentation, however, is to call attention to a sleeper making an end run on clever semantics and sophisticated technology.

The things I shall speak of are directly from the public record; some are inferential, some from first-hand experience. I will not disclose classified information not in the public record.

THE BATTLEFIELD

In order to develop my subject, let me direct your attention to the scenario of a battlefield in this newest kind of electronic warfare.

You have before you the roadmap of a typical electronic battlefield. This is the battle of Washington, D.C. The war is quietly being fought as we now sit in this chamber.

The terminals indicated by the crosses are A/T&T microwave long lines towers. The circles are those of the Chesapeake and Potomac Telephone Company, a subsidiary of AT&T. The hexagons belong to the Western Union Company.

Most long distance telephone calls travel across the country through a vast lattice of thousands of such microwave links.[3]

The great advantage of microwave transmission is its unusually broad bandwidth permitting large numbers of simultaneous talking circuits to exist on a single beam.

---

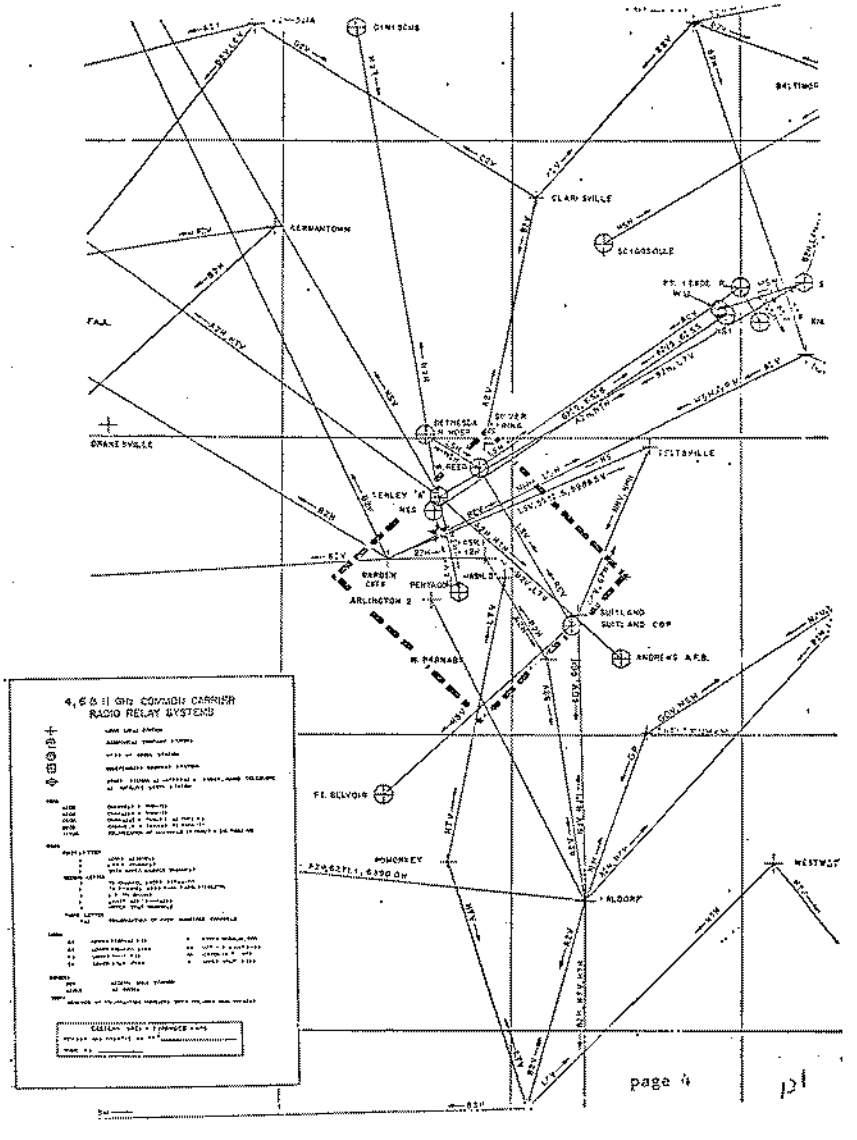
[1] Daniel Patrick Moynihan (D., N.Y.) press release, July 27, 1977.

[2] Congressional Quarterly, Weekly Report, vol. XXXV, No. 53, Dec. 31, 1977, p. 2687.

[3] Each microwave link, usually no longer than 15 to 25 miles in length, consists of antennas, transmitters, receivers, repeaters and associated equipment, employs highly directional, pencil beams of microwave radio energy. These beams, traveling in opposite directions between the terminals of the link, each carry the respective sides of telephonic conversations—those of the calling and called parties.

The super high frequencies of microwave carrier circuits are typically in the order of four, six or eleven gigaHertz (thousand-million cycles per second). Ordinary standard AM broadcasting at medium frequency is only about 1000 kiloHertz and FM broadcasting at very high frequencies is down in the region of 100 megaHertz (one hundred-million cycles per second).

The advantage of microwave communication becomes its weakness. By tapping into the microwave beam, the space-age eavesdropper immediately has access to thousands of conversations, data transmissions, and telegraphic messages.



A typical microwave link will have a multiple of 1800 voice channels in each direction.[4]

Esoteric electronic snooping into microwave circuits may be achieved at almost any geographical point within the beam paths.[5]

Movement of the Russian embassy to its new Washington, D.C. location on Wisconsin Avenue at Calvert Street will place the Soviets in an ideal geographical position for the interception of critical microwave telecommunications circuit paths used by the Pentagon and other facilities carrying national security information.[6]

This new vantage point, indicated by the star in the center of the microwave circuit map, will fix the extraterritorial eavesdropping facilities of the Russians directly astride two microwave beams each terminating in the "Garden City," Arlington, Virginia telephone tandem switching station. The opposite ends of these links each respectively terminate in Beltsville and in Gambrills, Maryland. One of these circuits is a primary North-South trunk line for the eastern seaboard and interconnects the Langley, Virginia facilities of the Central Intelligence Agency with Baltimore, Philadelphia, New York and Europe. The other circuit carries much of NASA's missile and satellite tracking and data information.[7]

---

[4] These voice channels are interleaved across the band spectrum in a hierarchy of subordinate groups and banks using an intricate technology known as multiplexing.

Each time a long distance call is placed, a pair of these multiplexed voice channels is occupied, one circuit in each direction. Before the communicating parties begin to talk, however, their conversation is preceded by a series of "address" multifrequency codes. This set of a dozen or so signals is the "beedle-de-beeps" heard in the background after dialing a long distance call. These tones identify the called number and cause the switching system to interconnect the desired parties. The technique of sending the multifrequency "address" tones over the *same* channel which subsequently will be used for talking is known as in-band" signalling. This technology is used almost exclusively across the country. It becomes especially useful to sophisticated interlopers.

[5] Such interception may also occur outside the path when a listening post is sufficiently near a microwave tower to pick up the spill-over energy in the side lobes of the antennas.

Using modern micro-electronic technology, the listening post may be completely automantic, unmanned, and no larger than an ordinary hi-fi receiver. The antennas need be no bigger than dinner plates, one facing in each direction to catch both sides of the conversations. The receivers are configured to separate the respective voice circuits, all 1800 lines, by the process of demodulation and demultiplexing. Each of these lines is continuously scanned by an associated micro-computer to detect the presence of certain "watch-list" multifrequency tone sequences—those corresponding to targeted telephone numbers of particular interest. The watch list may be changed daily or even hourly.

Further sophistication of the system may employ special programming permitting the targeting of any digital data message or telegram having key trigger words of interest. When a watch list telephone number or trigger word is scanned by the system, the whole body of the message is "dropped" into a tape recorder for further analysis.

[6] "Soviet Monitors Many Calls," New York Times, July 10, 1977; Burnham and Horrock.

[7] Strangely enough, the new Soviet site is also crossed by the microwave data circuit between the Pentagon and Western Union's "Tenley Tower" just off Wisconsin Avenue at Forty-first Street in the District of Columbia. The Tenley Tower microwave station is a primary junction point through which the Pentagon interconnects with virtually all national and international U.S. military establishments around the globe by means of its AUTODIN system (Automatic Digital Network of computers and teleprinters).

Also, because of its position and higher elevation, the new Soviet real estate will allow access to the two microwave circuits from the National Security Agency facility at Fort Meade, Maryland and the two corresponding terminals respectively at Tenley Tower and at the Naval Security Station on Nebraska Avenue near American University in N.W. Washington, D.C. The main beams of these latter two terminals outward bound toward Fort Meade do not pass directly over the new Russian embassy site. The transmitting antennas will be so close to the Russian listening antennas, however, that the radiating side lobes containing the targeted information may be detected and processed by the Soviets.

In like manner, the microwave link between Tenley Tower and the "underground pentagon" at Fort Richie, Maryland is in direct line with new Russian embassy facilities. Hence, another critical circuit becomes vulnerable to interception.

Plans are now underway to neutralize this vulnerability by scrambling messages, by reducing electronic accessibility, and by reducing physical accessibility through direct burial of coaxial cable.[8, 9, 10]

Enough is said here about the activity of foreign agents intercepting domestic telecommunications. Perhaps it is expedient that the discussion turn toward the main subject of this presentation, namely the interception of the communications of American citizens by the American intelligence establishment without benefit of court order under the criminal standard *or* under the non-criminal standard as proposed in several versions of S. 1566.

I ask you to look again at the diagram of the battle scenario. The microwave stations designated by circles all belong to the Chesapeake and Potomac Telephone Company. Each station is on a military facility. Among these are the National Security Agency at Fort Meade, the Naval Intelligence Support Center in Suitland, Maryland, and the Army Facility at Ft. Belvoir, Virginia. It may be seen also that there is an interconnection between this system and the local C&P Telephone Company circuits, and that there is an interconnection with the nationwide microwave domestic telephone system owned by AT&T.

The foregoing has little real significance taken by itself. The military require special high-volume circuitry, and at times it must interconnect with the national domestic system for service. The military must talk back and forth among its elements, both here and abroad.

The significance of the system shown interconnecting our domestic telephone system and the several secret military facilities is that a greater portion of these circuits are one way, receive only beams!

It is understandable that radio and television, weather and press wire communication services would require only one way circuits. It is not understandable that the National Security Agency would require thousands of times the circuit capacity of the world's press services combined. AP, UPI, Reuters, etc., except that these one way circuits are thousands of remote wiretaps!

---

[8] White House administrative background briefing, Frank Press and David Aaron, Nov. 18, 1977.

[9] Oh. Cit., N.Y. Times, July 10, 1977.

[10] The American Telephone and Telegraph Company and its subsidiary Long Lines Company have been requested to assist the federal government in reducing the vulnerability of microwave "earth" circuits to interception. The satellite communication carriers that also use microwave transmissions are being asked likewise to cooperate.

There is much talk of underground burial of high vulnerability or high density sensitive circuits by reverting to the coaxial cable technology of several decades ago, or to accelerate the plans for installing fiber optic. LASER circuits in critical areas.

Except for a few special cases. It is highly unlikely that the common carriers will succumb to pressure by the administration to change plans to go underground simply to achieve greater communications security. The cost would run into billions of dollars.

Rather, it is anticipated that the carriers will gradually shift to using special signalling, multiplexing, modulation, and routing and using schemes employing encrypting and scrambling. Intercepted information thereby becomes meaningless gibberish to the uninvited.

High among the security methods on the drawing boards is a technique known as Common Channel Interoffice Signalling (CCIS). AT&T, prior to the current security flap, had already planned to go this route for its own reasons. Contrasted with the present in-band signalling methods. CCIS is an out-of-band approach to the tasks of controlling the switching and routing of telephone calls.

Instead of transmitting the multifrequency tone code groups on the same channel containing the body of a message, namely the talking circuit, these "address" signals would be confined to a few designated channels set aside for signalling alone. Thus, the control signals for many different calls would be transmitted sequentially over a common channel between telephone offices, toll exchanges, and switching centers.

A snooping "microtapper" when attempting to discover a targeted watchlist telephone call by looking for its associated address codes in the CCIS system would experience an almost impossible task of locating the conversation of interest down among the voice channel stacks.

Further sophistication of the security system being considered is to encode the multifrequency signals so that the tapper will not only lack ready access to the communication of interest, but he will also be denied access to the "fact" that a called target telephone number has passed through the microwave link.

An additional twist to the approaches being considered is to periodically and randomly change the positions of each side of two-way conversation within the channel bank multiplex interleaving so that the wiretapper going barefooted on a blind prowling expedition through the voice channels would find it virtually impossible to match up both sides of any conversation.

The Data Encryption Standard (DES) developed by the National Bureau of Standards in the past few years is an encoding scheme for the transmission and storage of digital data, computer information, and telegraphic messages. Telex and TWX. The mathematical algorithm of the DES is built into a small integrated circuit chip similar to those used in pocket electronic calculators. The DES chip when installed in a computer data transmission terminal or even a simple teletype machine will provide considerable privacy to information sent from and between these devices.

By way of illustration, I have just described two means of the broadband interception of telecommunications circuits, one by interposing a receiving device into microwave beams, the other by direct, hardwire interconnection with our telephone and telegraph systems.

I believe there is substantial evidence to show that wholesale wiretapping of these peculiar types is being done in the United States by our own intelligence services, and that ordinary citizens who have nothing to do with the business of spying or espionage are thereby regularly having their privacy invaded.

I believe there is evidence to show:

(*a*) That Operation Shamrock to this date continues to operate under another name and another technology. (See p. 167)

Shamrock, a broadband interception of sorts, was that practice wherein the NSA and FBI were secretly and visually reading virtually every telegraph cable message entering or leaving the U.S.A. for the past thirty years. This practice was discontinued after discovery by the Senate Committee. Such practice was considered to be in violation of the Communications Act of 1934, the current title III wiretap law, and the Constitution itself. Now, however, there is reason to believe that the NSA is using the domestic and international communications long line systems, primarily the microwave networks, to accomplish the same examination of cables once attainable through **Shamrock,**

(*b*) **That the NSA has tacitly assumed and secretly taken the position that** no ordinary citizen has the right to communicate truly private messages through our telephone and telecommunications systems—messages which cannot be understood or read by the federal government. (See pp. 172, 173, 174, and 175.)

This is tantamount to the Post Office decreeing that henceforth no sealed envelopes may be mailed—only postcards may be sent which are easily read by the postal service.

(*c*) That the growth of surveillance technology is moving faster than the making of laws to control it.

(*d*) That there is reason to believe that the NSA continues to discolor and misrepresent to Congress the true effectiveness of its mission and the main bulk of its activity, and

(*e*) that the NSA continues to threaten and intimidate research scientists and American industry involved in telecommunications and information transmission through backhanded, extra-legal means.

I wish to return to the first assertion, namely the continuance of Operation Shamrock.

It appears that the positions taken by our intelligence community in general, and the National Security Agency in particular, regarding the use of broadband interception practices and the interception of non-oral communications, techniques which are particularly applicable to the microwave systems, are highly questionable in the terms of the Fourth Amendment to the Constitution.

There is no significant difference between electronic broadband interception practices and the early practice wherein agents of the Crown of England, during colonial times, armed with general warrant documents or writs of assistance, could plunder at random through the homes, offices and effects of citizens and could read, examine or carry off any document or property thought to be in the interest of the King.

Lord Camden, in 1765 condemned the general warrant, and struck it down through the courts.[11]

In his famous dissent, Justice Brandeis wrote of government wiretapping that ". . . writs of assistance and general warrants are but puny instruments of tyranny compared with wiretapping."[12]

Yet, by sweeping through our telecommunications system, looking for trigger words, multifrequency address sequences, or peculiar data patterns, all part and parcel of our private messages,[13] the National Security Agency, in effect, is searching through the private effects of thousands of untargeted citizens in order to secure targeted objectives.

This is the same as if the FBI were to go down your street, house by house, enter your home, search through your private correspondence, and by reading only the outsides of envelopes and file folder tabs, would make judgements of whether there is a scintilla of a doubt that you are a loyal American, or that you

---

[11] *Entick v. Carrington*, 1765.
[12] *Olmstead v. United States*, Supreme Court, 1928.
[13] See definition of "Contents", title III U.S.C., chapter 119, § 2510.

are engaged in activity that they, for one reason or another, thought you ought not to be involved in. All of this searching would be done because someone on your street, under the remotest possibility, might be a foreign agent.

Not a person here would stand for such a physical search without the issuance of a judicial warrant on probable cause that a crime is involved. You would not permit the search even if you had nothing to hide. Who among us does not have something that should be kept private? You would not permit an unwarranted search even if the FBI promised they would not "take" anything, just look.

For some strange reason, however, there is less reluctance among us to allow electronic searches through our telecommunications if we just don't know about it.

It appears that the intelligence agencies are using the cloak of secrecy and the mystique of technology to cover up practices which are becoming fairly evident to any one who will study into the subject.

There is great doubt that the U.S. intelligence community is hiding any really significant intelligence interception methods and techniques from the Soviets or any of the other nations of advanced technology.

Only the people of the United States, the courts and the legislative bodies are being kept in the dark or in a state of confusion.

The roots of these assertions are exposed in the hearings on S. 1566, in the oral testimony, and in the text of the bill itself.

NO CITIZEN TARGETED

According to Director Clarence Kelly of the FBI, Rear Admiral Bobby Inman of the National Security Agency[14] and Attorney General Griffin Bell,[15] "no citizen is targeted" for electronic spying within the United States as of June 9, 1977 under the general rubric of foreign intelligence.

This cryptic stock response sidesteps the direct question put by Senator Edward Kennedy and others as they attempt to find out if there are any "U.S. citizens that are at the present time, subject to electronic surveillance . . . ?"

It is curious to observe that on these and other occasions the federal law enforcement and intelligence enclave "just happened" to have terminated surveillance programs only a few days or weeks before they were brought up before Congress. Such practices were stopped, we are told, with no explanation of why it was necessary to continue them for so long, nor why they suddenly became unnecessary.

These intelligence agencies continue to this day to dance around the direct question of electronic surveillance of U.S. citizens. Pressed for further clarification of the stock phrase "no citizen is targeted", they respond with an equally stock retort that it is not possible to discuss this inasmuch as it deals with classified intelligence methods and techniques.

The clever usage of the phrase "acquired by intentionally targeting that United States person" is perpetuated in S. 1566 under definition (6)(A), § 2521. The key word is "targeted," not" intercepted". It is recommended that this unfortunate phrase be stricken and in lieu thereof the words added:

"The acquisition by an electronic, mechanical or other surveillance device of the contents of any wire or radio communication sent or intended to be received by a particular United States person where the contents are acquired under circumstances in which a person has a reasonable expectation of privacy."

In actuality, the technology being employed identifies targeted trigger words in thousands of telegraphic or data messages, or identifies peculiar signals associated with telephone calls as they pass through the dragnet. An automatic recorder then snatches out the whole message for later examination by agents. Thus, it is not "persons" who are the primary targets of these insidious kinds of surveillance, rather it is "information" which is targeted. Small consolation that the private communications of innocent citizens are sucked up into the NSA vacuum cleaner![16]

The Supreme Court declared that wiretapping, the interception of common carrier telecommunications, falls under the search and seizure protection of the

---

[14] Hearings, Senate Judiciary Subcommittee on Criminal Laws and Procedures, June 13, 14, 1977, on the Foreign Intelligence Surveillance Act of 1977.

[15] Hearings, House Select Committee on Intelligence, Jan. 10, 1978, on the Foreign Intelligence Surveillance Act of 1977.

[16] Science Magazine, AAAS, "Telecommunications Eavesdropping on Private Messages, p. 1061, 9 Sept. 1977.

Fourth Amendment to the Constitution, and that national security taps, as any other wiretap, must conform to court ordered warrant requirements.[17, 18]

On their own authority, however, a small inner circle of Defense and Justice department employees have chosen to interpret the court rulings and current laws to mean that certain esoteric kinds of wiretapping are excluded from constitutional guarantees.

This inner circle is similar to the *cabenet noir*, the black chamber established by Louis XIV of France and which continued through the Fifth Republic. During this time the private correspondence of the mails of France were regularly intercepted and read by this institution even though public law specified the death penalty for such violation.[19, 20]

Further evidence of the broadband sweeping of multicircuited domestic telecommunication trunk lines such as are contained on terrestrial and satellite microwave beams is hidden among the amendments to title III, chapter 119, the current wiretap law, by S. 1566 and its predecessor S. 3197. A stipulation is inserted therein which will permit warrantless wiretapping "for the sole purpose of determining the capability of equipment" when such "test period shall be limited . . . to . . . ninety days."[21, 22, 23]

Let there be no misunderstanding here. There is only one category of wiretapping equipment or system which requires up to ninety days for test and adjustment, and that system is broadband electronic eavesdropping equipment, the vacuum cleaner approach to intelligence gathering, the general search of microwave trunk lines. I make this assertion on the strength of actual experience in the electronic intelligence trade and on the strength of over twenty-five years experience in the telecommunications profession. An ordinary, single line wire tap requires only five minutes to adjust and test.

Additional roots of the attempt in S. 1566 to achieve warrantless wiretapping through the clever use of "secret" language are traced through the stipulation of the first sentence of the Act. Herein the definitions of the current wiretap law, chapter 119, are made to apply to the proposed statute in chapter 120. It is stated that "Except as otherwise provided in this section the definitions of section 2510 of this title shall apply to this chapter."[24]

Through this loophole, a most dangerous root is being drawn into S. 1566. This is found in the definition of "Intercept" stated to be "the aural acquisition of the contents of any wire or oral communication through use of any electronic, mechanical, or other device."

The inclusion of the word "aural" to the exclusion of any other kinds of acquisition has introduced untold confusion in the courts, and the legal profession in general. By excluding "nonaral" communications from the wiretap law, the NSA, the FBI, and other intelligence agencies have justified the warrantless wiretappings of citizens for years. In fact, it could be reasonably argued that any citizen could engage in warrantless wiretapping of the nonoral variety with impunity.

It must be understood that the nonoral, nonaural proviso excludes digital telegraphic messages such as Telex, TWX, telegrams, cables and such other similar data as missile telemetry, video television, facsimile, banking, business, credit, insurance and medical information. It also excludes switching and signalling information used in the routing and billing of telephonic and telegraphic circuits.

The House Judiciary Subcommittee on the Courts, Civil Liberties and the Administration of Justice, known as the Kastenmeier subcommittee, has unanimously chosen to strike the word "aural" from the Chapter 119 definition of "intercept". By this they intended the wiretap law to include nonoral "textual" information such as in telegrams, but also nonoral "address" information such

---

[17] *Katz v. United States*, The Supreme Court, 1967.
[18] *United States v. United States District Court*, The Keith Case, Supreme Court, 1972.
[19] Report No. 30, Senate of the French Republic, Minutes of October 25, 1973, The Committee to Oversee the Public Services Conducting Wiretapping.
[20] See also, The American Black Cabinet, p. 22 this report.
[21] Senate Report No. 94–1035, S. 3197 The Foreign Intelligence Surveillance Act of 1976, Committee on the Judiciary; p. 3 amending U.S.C. Title III, ch. 119, § 2511(2)(c); also p. 178.
[22] Hearings, Senate Judiciary Subcommittee on Criminal Laws and Procedures on S. 1566, 95th Congress, June 13, 14, 1977, p. 157.
[23] Senate Report No. 95–604, S. 1566, The Foreign Intelligence Surveillance Act of 1977, Committee on the Judiciary, p. 69.
[24] *Ibid*, p. 72.

as included in communications signalling—the kind captured by the pen-register device.[25, 26]

The staff of the Senate Select Committee on Intelligence have indicated that they intend that nonoral communications shall be included in the coverage of S. 1566.

The mere striking of the word "aural" from the definition of intercept, however, is not explicit enough to retard the scanning of the nonoral components of trunk lines and microwave transmissions. There is too much danger of our waking up thirty years hence and discovering that what we thought was covered by the language was not covered at all, and that we have had thirty years of abusive surveillance.

Better language for the definitions may be found in the "Telecommunications Privacy Act of 1977" H.R. 7139.[27]

Incidentally, the legislative and judicial history of the use of the pen register, a type of interception device using nonoral communications, is fragmented with erroneous assumptions and technical inaccuracies. These inaccuracies have persisted from the first landmark case[29] occurring after the passage of the wire-

---

[25] The Bill of Rights Procedures Act of 1977, HR 214, HR 215, S. 14.

[26] The simplest, most widely used, and perhaps the oldest switch and signal wiretapping device employed is the so-called "pen register." This type of device is known to have been used widely for several decades. It is connected across the telephone line of a subscriber in a local exchange or anywhere in the line between the subscriber's handset and the local exchange and will "record" the digits of all ontgoing telephone numbers dialed from the telephone.

The pen register will record both local and long distance outgoing calls. It will identify all subscriber dialing action even if the telephone of the dialed party is busy, or out of service, or not unswered. It has an advantage over using telephone company billing records as a source of intelligence since it captures the local calls, incomplete calls, and no-charge toll calls ("800" prefix calls) not recorded on the telephone bill. An additional advantage of this device over using telephone company billing records is that when coupled with a clock timing device, the pen register will provide a record of the exact time each telephone call is placed.

A further advantage of the pen register technique to the investigator is that it may involve only one technical person in a telephone exchange for installation, and thereby avoid the labyrinth of officials and clerks in the telephone business office, any one of whom may blow the whistle on the whole operation. The pen register, when installed on the line between the exchange and subscriber's telephone handset, need not involve anyone in the telephone company but rather only an agent representing whatever governmental ageney is performing the tapping operation.

The pen register connection to a telephone line or gronp of lines often is used as a "sieve" to gather intelligence which will further direct an investigating agency to an area wherein they may wish to apply other pen registers or actual "audio" intereeption wiretaps.

Again, under present rulings, the use of the pen register does not fall nnder the purview and control of the wiretap laws, namely Title 18, Chapter 119.

[27] Telecommunications Privacy Act of 1977, HR 7139, Rep. Kildee (D) Mich., May 12, 1977, p. 23–24. "Intereept means (to) acquire—by means of any device—a transfer of verbal, symbolic, or other information between persons or information processing facilities, including associated switching and signalling information—

(A) That is made in whole or in part by wire, cable, microwave radio, satellite, or an optical system furnished or operated by a communications common carrier;

(B) That is made on a private communication system; or

(C) That is an oral communicaiton uttered by a person having an expectation in circumstances justifying that expectation that such communication is not being intercepted."

[29] It is interesting to note that the first landmark case involving the use of the pen register which occurred after the establishment of the current wiretap laws as described in the Omnibus Crime Bill was decided upon against the defendent. His telephone line was tapped using a pen register without a warrant or without Attorney General permission. The case was not ruled upon as a matter of his constitutional rights. Nor was the issue one which questioned whether switch and signal intercept wiretapping was, in fact, an interception under the definition of Chapter 119. Rather, the ruling was made on the basis that one of the parties to the conversation, the receiving party, had given permission for the device to be placed on the circuit.

"Where pen register was attached by telephone company to defendant's telephone line with knowledge and consent of recipient of threatening calls, evidence that calls were made from defendent's telephone to recipient's telephone did not violate this section (2515) prohibiting the unauthorized intereception and divulgence of any telephone communication. *State* v. *Holiday*, Iowa 1969 N.W. 2d 768."

It is clear that the point of law and the thrust of the argument is directed toward the statement of § 2511(2)(c) which reads:

"It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception."

Certainly making threatening telephone calls was and is probable cause to investigate such behavior. And, if evidence is in hand, legally obtained, it can be brought before the courts, and the plaintiff is justified in bringing action against the defendent.

We object in this case, however, to the method of obtaining the pen register evidence, and the justification for the admissibility of such evidence. Apart from our objection to the dismissal that this kind of wiretap, the switch and signal sort, is not really a wire

tap law in 1968 up through a Supreme Court case just heard and ruled before the first of this year.[29]

The main argument of the recent Supreme Court case to exclude the pen register from the controls of the wiretap law was that the word "aural" in the definition of "intercept" limited the coverage to oral communications.

The legislative history of the insertion of "aural" into the "intercept" definition shows that it was thought that pen registers were used in the tracing of telephone calls.[30] This is simply not the way telephone calls are traced. The pen register is a surveillance device put directly on the telephone line of a known suspect, or suspicious pay phone, only after that suspect or instrument has already been traced by other means.

The dangerous aspects of allowing this procedure to occur outside the control of the wiretap laws is that the language of these significant court cases use the phrase, "pen registers, and like devices." The "and like devices" opens up the gate for a host of unspecified surveillance devices which scan non-oral communications, Telex, data, multifrequency tones, and switching and signalling functions; operations occurring on broadband trunk lines such as our toll microwave circuits.

The real issue of the Supreme Court pen-register case is that the current practice of instituting this kind of surveillance involves obtaining a court order under Rule 41 of the All Writs Act of 1789, *vis-a-vis* the obtaining of another kind of court order under the Omnibus Crime Bill, wiretap law of 1968.

Other than the fact that a Chapter 119 wiretap order is a mite more difficult to obtain—the probable cause requirements a bit stiffer—why all this fuss? A court order is a court order.

The bottom line significance of this whole case has never been articulated in public. The significance hinges on the reporting requirements of the wiretap law.

Apparently, there is great pressure from subterranean halls to prevent the assemblage in one place complete and accurate records of the scope and magnitude of the clandestine use of pen registers and like devices on the American populace.

The wiretap law would require that such records be sent to the Administrative Offices of the Courts in Washington, D.C. Here it would be available for examination by Congress. Reduced and sanitized statistical data would be available to the public.

Such devasting news would become almost unbearable. Some have estimated that the numbers of telephone and telegraphic messages within the United States that are "scan" intercepted per year run into the billions. There are no public records yet to that affect.

In an earlier testimony on S. 1566 before the Senate Judiciary Subcommittee on Criminal Laws and Procedures, it was recommended, as a Minimization Criterion, that broadband interception for both criminal and intelligence purposes be made unlawful altogether.[31]

The acquisition of the targeted information may be effected on single telephone lines; albeit with slightly more difficulty. It was further recommended that all types of non-oral communications, including switching and signalling, be included in the warrant protections of the current wiretap law and in S. 1566.

---

tap; apart from our objection to the dismissal that no warrant was needed for the interception of this kind of wire communication; and apart from our objection to any kind of wiretapping under any premise; we find that the argument used by the court shows a lack of understanding of the most elemental operation of a telephone system.

The pen register device was not connected to the telephone line of the recipient of the threatening telephone calls, but rather to the line of the defedent. It may be argued that these lines were all the same line once interconnection was established. This, under the most extreme stretch of ones technical imagination, may be true. But the pen register "recording", however, was not made at a time when the defendant's line was connected to the line of the recipient. The interconnection between lines was accomplished only *after* the last pulse of the last digit of the dialed telephone number was dialed by the defendent.

Apparently the courts, in this case, were unaware of the temporal conditions of telephone interconnection, and the time the pen register recording was made, or the courts chose to ignore these facts.

In most cases of the use of pen registers, no parties to the communication have given permission for the recording to be made.

[29] *U.S.* v. *New York Telephone Co.*, Supreme Court, cert No 76-835.

[30] Ibid, U.S. Petition for Writ of Cert, appendix A, p. 4A.

[31] "Minimization Criteria", Testimony D. L. Watters, Sen. Jud. Sub. on Criminal Laws, S. 1566, 14 June 1977.

Let there be no mistake. Tons of electronic surveillance equipment at this moment are interconnected within our domestic and international common carrier telecommunication systems. Much more is under contract for installation. Perhaps this equipment is humming away in a semi-quiescent state wherein at present "no citizen is targeted;" simply scanned. Its builders are lying low during the present critical time when embarrassing questions are being asked. How soon will it be, however, before a punched card will quietly be dropped into the machine, a card having your telephone number, my telephone number, or the number of one of our friends to whom we will be speaking?

What will happen when there is some international emergency, the firing of a nuclear device, the change of political perspectives, and, as a result, the full force of the electronic surveillance monster is unleashed? By comparison, the internment of American citizens of Japanese ancestry during World War II will seem like a Sunday school picnic.

We simply cannot continue such programs of building electronic surveillance systems simply because it is possible, because we have the technological capability and the financial resources. It is better that we pull the plug and disassemble much of the equipment already in place.

In recent testimony on this subject before the Michigan State Judiciary Committee, a prominent member of the White House Office of Telecommunications Policy said:[32]

"The time is here to begin to impose meaningful restrictions before the potential for damage becomes irreversible. Much of the applicable law regarding protections against interceptions rests on what is called the 'expectation of privacy' when such expectation is deemed reasonable. It could be at least theoretically interpreted that as a consequence of this declining expectation, the legal protections I would normally have are also declining. In other words, Catch-22; the more you know about the problem, the less protection you have to prevent it from happening to you.

"My personal concern and attention are mainly centered on the future; the next five to ten years. That is not to say that some of the present and past practices are not abusive. It only means that I fear the future will be much worse.

"There is . . . serious question about whether electronic interception of a private communication is inherently an unreasonable search and whether it is thus unconstitutional under the Fourth Amendment. This argument stems from the basically random nature of the typical electronic surveillance activity. . . . Given the seriousness of that problem today, how much more pervasive and intrusive will this kind of 'snooping' become in the future when the intercepting party has immediate access to greatly increased amounts of even more sensitive information than is available at present."

The National Security Agency

The federal intelligence agency of prime concern here is the National Security Agency (NSA). Official published estimates of its size in dollars expended or manpower employed, by either the Legislative or Executive branches, do not exist.[33] Unofficial estimates are that the NSA annually spends as much as $15 billion and employs up to 120,000 persons, when military agencies under the

---

[32] Michigan State Senate Judiciary Committee, testimony, T. J. Steichen, regarding wiretap legislation, 18 May 1977.

[33] The House Select Committee on Intelligence (hereafter cited as Pike Committee) noted that the total annual intelligence community budget was "more than $10 billion;" that the NSA "has one of the largest budgets in the intelligence community;" that "roughly 20 percent of the National Security Agency's budget is not added into the intelligence budget;" that "the costs given Congress for military intelligence (much of which would be applicable to NSA's functions) do not include expenditures for tactical military intelligence, which would approximately double intelligence budgets for the three military services." (Pike Committee Report, Village Voice, February 16, 1976, p. 72.)

This appears to conflict with a CIA briefing given to President-elect Jimmy Carter, that "the military branches of the intelligence community receive more than 80 percent of the roughly $4 billion budgeted annually for *all* United States intelligence efforts, principally for the photo reconnaissance and radio signals interception technology used to monitor potential adversaries." (David Binder, "U.S. Intelligence Officials Apprehensive of New Shake-Ups Under Carter." New York Times, December 13, 1976, p. 43 Empbasis added.)

NSA's direction are included.[34] Whatever its actual budget and personnel levels, it has, through a network of over 2,000 specialized intercept positions around the world, the technological capability to intercept a significant portion of all telecommunications, world wide. This capability can be brought to bear against any country. If used against the American people, Senator Frank Church has noted, "no American would have any privacy left . . . there would be no place to hide."[35]

The NSA was created by a seven-page Top Secret memorandum from President Harry S. Truman to Secretary of State Dean G. Acheson and Secretary of Defense Robert A. Lovett, on October 24, 1952. Under this directive, which even today remains classified, the NSA assumed the responsibilities of the Armed Forces Security Agency, which in turn had largely inherited the intelligence responsibilities of the Army Security Agency (which even yet remains a functioning Army entity).[36]

The NSA's two basic functions, derived from Top Secret National Security Council and Director of Central Intelligence directives, are: (1) to protect the "Communications Security" (COMSEC) of U.S. telecommunications that are national security related; and (2) to obtain foreign intelligence related telecommunications through the interception of "Signals Intelligence" (SIGINT).

The SIGINT interceptions are the NSA's dominant operational activity. It consists of "Communications Intelligence" (COMINT), which involves the interception of electronic message communications (such as telegrams and telephones) and "Electronic Intelligence" (ELINT), which involves the interception of signals (such as radar and missile emissions).

Here we are primarily concerned with the NSA's COMINT activities in areas of non-oral and broadband telecommunications,[37] as they affect the constitutionally guaranteed right of privacy of American citizens. We also note, to a lesser extent, one COMSEC activity that extends beyond the "protection" of communications related to national security, that may likewise encroach on the privacy of American citizens.[38]

PRE-WORLD WAR II INTERCEPTION OF NON-ORAL COMMUNICATIONS

During World War I, U.S. government intelligence agents censored telegraphic telecommunications by working in the offices of private telegraph companies; all messages entering or leaving the United States were at the disposal of a military intelligence unit of the War Department known as MI–8 (Military Intelligence—Section 8).[39] Unlimited government access to messages ceased when cable censorship by U.S. authorities was discontinued in late 1918 and early 1919.[40]

MI–8, from its inception in 1917, was directed by Herbert Osborne Yardley, considered by some cryptologists to be the most famous in history. At war's end,

---

[34] David Kahn, author of "The Codebreakers," a definitive work on cryptology, describes the NSA as "the largest and most secretive of all American intelligence organs," and estimates that on its own it "spends about $1 billion a year." But, he adds, "the agency also disposes of about 80,000 servicemen and civilians around the world, who serve in the cryptologic agencies of the Army, Navy, and Air Force (that) stand under NSA control, and if these agencies and other collateral costs are included, the total spent could well amount to $15 billion." (Source: David Kahn, "Big Ear of Big Brother", New York Times Magazine, May 16, 1976.)

Tad Szulc describes NSA as "the largest, most important, most expensive, and secret member of America's 'intelligence community,'" which "costs over $10 billion a year and employs some 120,000 persons around the world." According to Szulc, "a vast array of specialized military agencies such as the ASA (Army Security Agency) the USAFSS (United States Air Force Security Service), and the NSG (Naval Security Group) . . . account for the vast majority of NSA's military and civilian employees." Approximately 90 percent work abroad. (Tad Szulc, "The NSA—America's $10 Billion Frankenstein", Penthouse, November 1975.)

[35] "Meet the Press" interview, August 17, 1975.

[36] See footnote 34.

[37] "Non-oral" as interpreted here includes cablegrams, radiograms, telex transmissions, computer transmission (such as used by banks for financial transfers), facsimile and video transmissions, telemetry, and telephonic switching and signalling control sequences (associated with telephone calls).

[38] From studies by the House Government Operations Committee, circa 1977–78.

[39] Army Security Agency, "Historical Background of the Signal Security Agency," Vol. III, p. 74; prepared under the Direction of the Assistant Chief of Staff, G–2, April 12, 1946.

[40] *Ibid.*

faced with the phasing out of his organization, and envisioning it having a peacetime role, Yardley, in May 1919, convinced the State and War Departments to jointly approve a plan for a "permanent organization for code and cipher investigation and attack." [42] Forty thousand dollars of the organizations $100,000 annual budget came from State Department special funds, the balance from Congress after military intelligence officials had taken selected Congressional leaders into their confidence.[43]

Although supported by government funds, the resulting organization had no visible government connection. Known as "The Black Chamber" by the few persons familiar with its existence, it operated from 1919 until 1929, under Yardley's leadership in New York City—under the cover name, "Code Compilation Company." [44] The operation was initially situated in townhouses in the East Thirties; following a 1925 break-in in which desks were rifled, it was moved to a large Manhattan office building.

In 1929, President Hoover's newly appointed Secretary of State, Henry L. Stimson, was shocked to learn of the Black Chamber's existence and abruptly terminated the operation [45] in the belief its activities were shameful in a "world [that] was striving with goodwill for lasting peace." [46]

Suddenly without a job and in need of funds, and believing that since the Black Chamber had been destroyed there was no valid reason for withholding its secrets, Yardley published "The American Black Chamber" in 1931, an international best-seller which described his organization's accomplishments. Translated into several languages, Yardley boasted:

"We solved over forty-five thousand cryptograms from 1919 to 1929, and at one time or another, we broke the codes of Argentina, Brazil, Chile, China, Costa Rica, Cuba, England, France, Germany, Japan, Liberia, Mexico, Nicaragua, Panama, Peru, Russia (sic), San Salvador, Santo Domingo, Soviet Union and Spain." [47]

The Black Chamber, he stated,

"Also made preliminary analyses of the codes of many other governments. This we did because we never knew at what moment a crisis would arise which would require quick solution of a particular government's diplomatic telegrams. Our personnel was limited and we could not hope to read the telegrams of all nations." [47]

Despite his proclivity towards sensational disclosures, Yardley coyly avoided stating how, in the ten years of MI–8's peacetime existence, from 1919 to 1929, the Black Chamber had obtained telegrams it had analyzed:

"We employed guards, replaced all the locks and were ready to begin (in 1919) our secret activities. But there were now no code and cipher telegrams to work on! The cable censorship had been lifted and the supervision of messages restored to the private cable companies. Our problem was to obtain copies of messages. How?

"I shall not answer this question directly. Instead I shall tell you something of the Soviet Government's type of espionage as revealed by documents that passed through our hands. After you read these, you can draw your own conclusions as to how the United States Government obtained the code and cipher diplomatic messages of foreign governments." [48]

However, this question was answered in a letter Yardley sent to his publisher on March 18, 1931; he wrote that none of the messages alluded to in the manuscript of "The American Black Chamber."

"Other than certain wireless messages exchanged between Germany and Mexico, were sent by radio. They came by cable. With respect to every cablegram referred to in such book, the copies thereof to which I refer therein were obtained

---

[42] David Kahn, "The Codebreakers" (New York, The Macmillan Company, 1967), p. 344.
[43] Herbert O. Yardley, "The American Black Chamber" (Indianapolis, The Bobbs-Merrill Company, 1931), p. 240.
[44] Army Security Agency, op. cit., p. 48: "In order to conceal the true nature of its activity, the office was called 'Code Compilation Company', a cover name for MI–8 but the real name of an incorporated business firm established by Yardley and Charles J. Mendelsohn, partners in this venture. This firm produced and sold in fairly large quantity, a code called the Universal Trade Code."
[45] Yardley, op. cit., p. 370.
[46] Quoted in Kahn, op. cit., p. 360n. (In this regard, Secretary Stimson also made his well-known declaration, "Gentlemen do not read each other's mail.")
[47] Yardley, op. cit., p. 332. (This forty-five year old list is not dissimilar to one possessed by Western Union International which, when subpoenaed by the House Gov. Ops. Committee on February 4, 1976, prompted President Ford to attempt to extend the so-called "executive privilege" doctrine to a private corporation).
[47] Ibid.
[48] Yardley, op. cit., pp. 240–41.

by the consent and authority of the respective presidents of the Western Union Telegraph Company and of the Postal Telegraph Company over the wires of one or the other of such companies such messages were transmitted."

In the 1920's, these two companies carried almost all the telegraphic communications in and out of this country.[49]

According to Yardley's book, only coded messages were turned over to MI–8; plain text (i.e. uncoded) messages were never intercepted.[50]

MI–8 apparently obtained coded messages in the form of printed telegrams or paper tapes which were to be transmitted or had been transmitted either by radio or by undersea cable. Presumably, at the time the "interception" was made, MI–8 would not have known which means of transmission would be used to carry the messages, nor presumably, would it have cared. It is problemmatical, therefore, whether existing legal restrictions on the use of interception of wire communication or radio communication would apply to these interceptions.

The Army Security Agency's 323-page "Historical Background of the Signal Security Agency 1919–1939," in sanitized form, omits any mention of the arrangement described by Yardley, whereby MI–8 received telegraph messages from the Western Union and Postal Telegraph companies, or any other company. This document states that:

"Plans for establishing MI–8 on a peacetime basis in 1919 included no provision for the development of facilities for obtaining the necessary intercepted messages. A detailed account of the situation will be given shortly but at this point it will suffice to indicate that it was doubtless assumed that the cable companies would continue to supply copies of all messages passing through their offices and that the Signal Corps would continue its war-time intercept facilities which would be at the call of MI–8. These assumptions proved to be unwarranted. That no satisfactory solution for this problems was ever reached was one of the prime causes for the decline of activity of MI–8 in New York. It was also one of the factors which led to the absorption of the Bureau of the Signal Corps, an organization which could more easily develop intercept facilities."[51]

No "detailed account of the situation" *vis-a-vis* the telegraph companies participation has yet been made available. Nevertheless, Yardley's account indicates MI–8 did become operational with the cooperation of the two telegraph companies identified above.

The factor leading to MI–8's demise was Secretary Stimson's philosophical and moral objections, not the telegraph companies' reluctance to make messages available.

When World War I ended, the Radio Communications Act of August 13, 1912, which provided that the Government would guarantee the secrecy of communications, was still in effect. That act provided, in pertinent part, that:

"No person or persons engaged in or having knowledge of the operation of any station or stations shall divulge or publish the contents of any messages transmitted or received by such station, except to the person or persons to whom the same may be directed, or their authorized agent, or to another station employed to forward such message to its destination, unless legally required so to do by the court of competent jurisdiction or other competent authority."[52]

This law did not prohibit the interception of radio traffic per se, but merely prohibited the employees of common carriers covered by the Act from the divulging or publishing of the contents of messages to unauthorized persons. It remained in effect until the enactment of the Radio Act of 1927, which considerably broadened the prohibition against unauthorized disclosures:

"No person receiving or assisting in receiving any radio communication shall divulge or publish the contents, substance, purport, effect, or meaning thereof except through authorized channels of transmission or reception to any person other than the addressee, his agent or attorney, or to a telephone, telegraph, cable or radio station employed or authorized to forward such radio communication to its destination, or to proper accounting or distributing officers of the various com-

---

[49] Postal Telegraph, the holding company controlling Commercial Cable, merged with Western Union in 1943. (Of the three U.S. companies now dominating the international telegraph business in and out of this country—ITT World Communications, RCA Global Communications, and Western Union International, an independent spin-off of Western Union—two were only minimally in the business in the 1920's, and one did not exist.)

[50] Yardley, op. cit., p. 342.

[51] Army Security Agency, op. cit., pp. 73–74.

[52] "An act to regulate radio communication," August 13, 1912, 62nd Cong., 2d Sess., Ch. 287, Statutes at Large, Vol. 37, Part I, p. 307.

municating centers over which the radio communication may be passed, or to the master of a ship under whom he is serving, or in response to a subpoena issued by a court of competent jurisdiction, *or on demand of other lawful authority;* and no person not being authorized by the sender shall intercept any message and divulge or publish the contents, substance, purport, effect or meaning of such intercepted message to any person; and no person not being entitled thereto shall receive or assist in receiving any radio communication and use the same or any information therein contained and no person having received such intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of the same or any part thereof, knowing that such information was so obtained, shall divulge or publish the contents, substance, purport, effect, or meaning of the same or any part thereof, or use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto. . . ." [53] (emphsis added)

Where as the 1912 Act applied only to employees of common carriers, the 1927 Act applied to all persons not authorized by the sender to receive such communications. The Army Security Agency's historical record states that the law's "or on demand of other lawful authority" provision was apparently never used to justify the interception of foreign diplomatic traffic.

Hence, subsequent to 1927 at least, the American Black Chamber apparently operated in violation of the law. The Army Security Agency's historical record suggests that the activities of military intelligence gathering—including MI–8's—were not intended to be covered by the 1927 Act's prohibitions:

"The purpose behind the legislation was of course the security of communications from the danger of interception by unauthorized persons who might have made use of intelligence contained therein for person profit. That the laws would also hamper Governmental agencies engaged in the production of intelligence upon which the safety of the United States might be based was probably far from the minds of legislators. Indeed, prior to World War I, no such agency existed, and until 1931, the fact that one had existed during the war period was unknown either to the general public or to most officers in the Army itself.

"On the other hand, inclusion in these acts of specific exemptions permitting the interception of radio communications for the purposes of military intelligence would have given notice to the world in general, and therefore to a possible enemy in particular, that cryptanalytic units were indeed operating. Such a course would have been highly undesirable. What solution this thorny problem could have had is not clear; the fact that no solution was ever reached constituted one of the greatest obstacles to the proper functioning of MI–8." [54]

Yardley infers that the 1927 Act presented no obstacle at all. It was simply ignored.

The 1927 Act remained in effect until it was superseded by the Communications Act of 1934.

The publication of Yardley's book, in 1931, prompted the War Department to state that the American Black Chamber had not existed for four years (a date which coincided with the passage of the Radio Act of 1927).[55] General Douglas MacArthur, then Army Chief of Staff, said he did not know anything about it. while high officers in the intelligence divisions said no such bureau then existed and they professed to have no knowledge of it in former years.[56] State Department officials similarly said they were sure there had been no such practice and one official speaking on behalf of Secretary Stimson, said he had never heard of any such organization as the so-called "black chamber." [57]

Yardley, a man who had been revered as a cryptanalytic genius, who, in 1922, had been personally given the Distinguished Service Medal by the Secretary of War,[58] was portrayed in official commentaries as an opportunist and braggart whose actions bordered on treason.

---

[53] "An act for the regulation of radio communication," February 23, 1927. 69th Cong., 2d Sess., Ch. 189. Statutes at Large, Vol. 44, Part II, Sec. 27, p. 1172.

[54] Army Security Agency, op. cit., p. 77.

[55] New York Times, June 2, 1931; p. 18.

[56] New York Herald Tribune, June 9, 1931.

[57] New York Times, June 2, 1931; op. cit.

[58] Yardley described his receiving the award, as follows:

"In awarding you the D.S.M.," the General began again, "we find it difficult to draft a citation that will describe your distinguished services, and at the same time keep the nature of your activities secret, for of course all citations are published. Have you any suggestions—"

"I naturally have never given the matter any thought."

"Well, we'll draft something so that your successor will not be revealed. The only regret is that the real reason for confirming the D.S.M. can not be given . . ."

The Army Security Agency history, written in 1946, described Yardley as a man who "had demonstrated a certain amount of cryptanalytic ability and had achieved within the War Department a reputation as a cryptanalyst." He was, the report stated, a poor administrator who had "neither the initiative nor foresight to build MI–8 on a firm foundation." He ignored his duties, the report continued, "while he profited from real estate activities; his enthusiasm for cryptanalysis lagged as he became a consultant in more profitable code production activities for commercial firms. Then, when his own position was abolished, he divulged information of the highest secrecy and made himself notorious in the annals of cryptology." [59]

In 1932, Yardley wrote a new book entitled "Japanese Diplomatic Secrets" that was never published. On February 20, 1933, U.S. marshals in New York seized the manuscript in the publishing offices of The Macmillan Company, on the grounds Yardley, as an agent of the U.S. government, had appropriated secret documents.[60] Yardley was never prosecuted, but to further counter him and others similarly inclined, the Congress passed, with State Department urging, the "Protection of Government Records" bill. Now codified as 18 U.S.C. 952, the bill made the disclosure of diplomatic codes or correspondence a felony.

According to the Army Security Agency's historical chronology, MI–8 primarily failed because "its principal support was derived from a department of the government which reflected political changes and the temper of the times more directly than does the War Department." [61] In other words, such a sensitive activity as MI–8 was not to be entrusted to the changing whims of the country's civilian leadership. The Army Security Agency, in hindsight, also saw other reasons for MI–8's demise:

"(1) The man most responsible for secrecy was the one who violated it (though there was no evidence Yardley compromised the "Black Chamber" in any way, during its twelve year existence).

(2) Its isolation from direct supervision as a result of its transfer to New York produced neither the desired secrecy nor the attention it should have had from the War Department (though there was every evidence, from Yardley's narration, its existence was well known at the highest State and War Department levels).

(3) The separation of cryptanalysis (breaking the codes and ciphers of foreign governments) and cryptography (making codes and ciphers for one's own government) was a mistake." (MI–8 was not involved in cryptography.)

Even before MI–8 formally terminated its operations on October 31, 1929, the War Department had formed the Signal Intelligence Service. By State Department default, most cryptological work was unified within the Army in a single organization [62]—a stepping stone to the evolution, in 1952, of the National Security Agency.

POST WORLD WAR II INTERCEPTION OF NON-ORAL COMMUNICATIONS

During World War II, U.S. government agents pursuant to the wartime powers of the President, again censored non-oral telecommunications by working in the offices of the telegraph companies. Three companies—ITT Communications, RCA Communications, and Western Union—transmitted almost all international cablegrams and radiograms entering or leaving the United States. All such messages were placed at the disposal of military intelligence.[63]

"I was to appear before Secretary of War Weeks at two P.M. to receive the D.S.M. On the way to his office I asked General Heintzelman if Secretary Weeks really knew why I was being awarded the D.S.M. He assured me that the Secretary was one of the most ardent supporters of the Black Chamber.

"I felt rather silly standing before the Secretary of War, as he read my citation that seemed to have very little to do with the breaking of codes of foreign governments, but I was relieved when he pinned the medal on my lapel, for with a twinkle in his eye he winked at me. The wink pleased me immensely." (Yardley op. cit., pp. 322–23.)

[59] Army Security Agency, op. cit., p. 177.

[60] New York Times, February 21, 1933, p. 3.

[61] Primarily from Army Security Agency, op. cit., pp. 176–80.

[62] The Navy also had its own cryptologic section. See Kahn, op. cit., pp. 386–88.

[63] ITT Communications is now ITT World Communications. RCA Communications is now RCA Global Communications. In 1963, Western Union's international operations were transferred to Western Union International, which was established as an independent company. Between 1971–1974, these three companies carried 94.9 percent of all international telegraph messages in and out of the U.S.

However, the War Department's post-World War II actions to convince the cable companies to make international telegrams available to federal intelligence agents were markedly different than those taken after World War I. The post World War I period was marked by inaction: six months after the Armistice, Herbert Yardley had to single-handedly persuade the government to enter into such an arrangement and his scheme provided that *only* coded messages would be handed over. But in August 1945, immediately after the end of the war, the Army Signal Security Agency, the same as the Signal Intelligence Service and the Army Security Agency, implemented a plan that led ultimately to making *most* telegrams entering and leaving the United States—including those in plain text—available to that agency.[64] On August 18, 1945, four days after Japan surrendered, "two representatives of the Army Signal Security Agency were sent to New York 'to make the necessary contacts with the heads of the Commercial Communications Companies in New York, secure their approval of the interception of all [foreign] Governmental traffic entering the United States, leaving the United States, or transiting the United States, and make the necessary arrangements for this photographic intercept work.' "[65] ITT and Western Union began their participation by September 1, 1945, and RCA by October 9, 1945.[66]

While the Army Signal Security Agency was ostensibly only interested in the interception of foreign government traffic, in practice it was given access to all traffic. This was necessary, former RCA Executive Vice President Sidney Sparks testified, because the procedures initially proposed by the government—that special electrical connections be put on certain tielines, or that tapes originating and terminating with certain tielines be turned over—would result in a situation where "everybody and his brother would know just exactly what we were doing and why."[67] To avoid that revelation, the government was given, according to Mr. Sparks, "all of the perforated tapes," i.e., access to all messages.[68, 69]

ITT also agreed to allow the Army access to all incoming, outgoing, and transiting messages—private as well as governmental—passing over the facilities of its subsidiaries involved in international communications. ITT agreed to

---

[64] In March 1976, when representatives of the three major American telegraph companies engaged in international communications testified before the House Government Information and Individual Rights Subcommittee, the subcommittee believed that the Government had not commenced its post World War II interception of private messages until 1947. This belief was based on a report issued by the Church Committee on November 6, 1975, at which time Sen. Church states:

"At meetings with Secretary of Defense James Forrestal in 1947, representatives of the three companies were assured that if they cooperated with the Government in this program, they would suffer no criminal liability and no public exposure, at least as long as the current administration was in office. They were told that such participation was in the highest interests of national security."

Shortly after the subcommittee's March 1976 hearings, a subcommittee staff inquiry led to records being uncovered in the Archives which indicated that the Army Security Agency had, in fact, taken steps to initiate the interception program as soon as the war ended. Prior to making these records available to the subcommittee, Archives sought Department of Defense permission; that permission was refused. The Department of Defense then advised the Church Committee of the existence of these documents, and allowed a staff member of that committee to inspect (but not copy) them. This transpired just prior to the issuance, in May 1976, of the Church Committee staff report on "National Security Agency Surveillance Affecting Americans," which was amended accordingly.

[65] Letter from Intelligence Officer of Army Signal Security Agency to Commanding General, August 24, 1945, quoted in Church Committee Final Report, Book III, pp. 767–68.

[66] Ibid, p. 769.

[67] Hearings, House Government Operations Committee, 94th Cong.; Oct. 23, 1975; Feb. 25, Mar. 3, 10 & 11, 1976; Interception of Nonverbal Communications By Federal Intelligence Agencies, p. 212.

[68] Ibid.

[69] Mr. Sparks, who was the most forthright of all telegraph company witnesses, testified that within RCA he was the sole authority for making all messages available to government agents, and that this arrangement began in 1947. There is no reason to doubt the accuracy of Mr. Sparks' testimony insofar as he was aware of the facts. The 1947 date, as he recalled it, was presumably a result of that being the program's generally accepted date of commencement, at the time of his testimony. His belief that he was responsible for making the arrangements with the government apparently is based on initiatives made to him by Army Security Agency representatives, subsequent to arrangements unknown to him being made with his superiors. (See October 9, 1945 letter from RCA Vice-President W. H. Barsby to Brig. General W. Preston Corderman, in Subcommittee Hearings, p. 208). Mr. Sparks apparently never knew about the 1947 meeting with Secretary Forrestal; Sparks' superior, Gen. Harry C. Ingles, then President of RCA Communications, represented the company.

The ITT delegation to the 1947 Forrestal meeting was led by ITT Chairman and President, Sosthenes Behn. Joseph L. Egan, Western Union President, was invited but did not attend, and his company apparently was not represented.

record . . . all such messages on microfilm, which the Army Signals Security Agency then developed.[70]

For the next thirty years, between 1945 and 1975, RCA and ITT—which together handled approximately 70 percent of all international non-oral telecommunications in and out of this country—continued to make all their customers' communications available to the NSA.[71] Only the form in which these messages were turned over changed during this thirty-year period.

Western Union's procedure was far more selective. It insisted from the time it entered into the program in 1945, that its own personnel do the actual handling of all messages delivered. Moreover only messages to one foreign country initially were made available to NSA.[72] At an undetermined later date, all foreign government telegrams were made available to NSA.[73]

Western Union's participation was also of shorter duration. In 1963, Western Union divested itself of its international operations, which were taken over by Western Union International, an independent company formed for that purpose. Sometime between 1965 and 1972, an NSA Recordak machine located in the company's New York operations room which company employees used to copy foreign government messages, was removed at the company's request.[74, 75]

There is no public evidence that, after World War II, the Army Security Agency—or, in 1952, its successor agency, the NSA—made any attempts to limit its "take" to coded messages from the telegraph companies, as was done by Herbert Yardley's MI–8 organization after World War I. Both coded and uncoded messages were received and analyzed, seemingly in violation of the 1958 National Security Council Intelligence Directive (NSCID number 6, dated September 15, 1958) setting out the functions of the NSA:

---

[70] Army Signal Security Agency letter, August 24, 1945, op. cit., p. 772.

[71] For a detailed description of these procedures see Church Committee Final Report, Book III, p. 765–776.

[72] Ibid., p. 775.

[73] Ob. cit., Gov. Ops. Hearings, p. 107.

[74] Western Union International's Executive Vice-President testified he had the machine removed in 1965. However, the Church Committee reported at Book III, p. 774: This recollection "was not borne out by documents furnished by NSA. The documents showed that on February 2, 1968, a company vice-president (not the one referred to above) had discovered the existence of NSA's Recordak (microfilm) machine in the Western Union transmission room. The machine was reported to the company president, who directed his employees to find out to whom the machine belonged. . . . It is clear that NSA continued to receive duplicates of all messages to the foreign country referred to above until 1972; when again as a result of 'discovery' by company officials, this procedure was halted. . . . In effect, Western Union International's participation in SHAMROCK ended in 1972."

On June 7, 1976, Mr. Greenish advised the subcommittee, through counsel ". . . that the practices discussed by him, copying foreign government traffic on the Recordak, terminated with the removal of the one and only Recordak 'about 1965.'" (Committee Hearings, p. 111.)

[75] In addition, the Western Union International office in London turned over communication entrusted to its care to the government of the United Kingdom. On March 3, 1976, Executive Vice President Thomas S. Greenish testified that his company never made cables available to authorities of any country other than the United States, but he subsequently told the Committee that he "misunderstood Ms. Abzug's question," and his attorney requested that his testimony be changed to show that messages had been turned over to British officials. (See Committee Hearings, pp. 112–13.)

Mr. Greenish's amended testimony is consistent with a February 21, 1967 report in the London Daily Express, which stated that telegrams sent out of Britain were regularly made available to that country's security authorities; the story noted that international telegrams which passed through foreign companies operating in Britain "are collected in vans or cars each morning and taken to the Post Office security department." On June 22, 1967, Prime Minister Harold Wilson told Parliament that the practice had been going on since 1927. On May 12, 1976, the British Embassy in Washington refused to state whether the practice continues, formally advising the Committee that "it is not in accordance with HMG's policy to comment on such matters."

On March 11, 1976, George Knapp, President of ITT World Communications, testified that to his "personal knowledge" his company had never made communications available to any foreign government. (See Committee Hearings, p. 306.) Representatives of RCA Global Communications were not asked if their company had ever made communications available to any foreign government.

The Congress does not know what uses the British government makes of the messages made available to it, nor does it know if the messages are disseminated to any other governments. The British government maintains a liaison office at NSA headquarters in Ft. Meade, Maryland, and the NSA maintains a liaison office at the British government's General Communications Headquarters in Sheltenham, 75 miles northwest of London. NSA personnel are also based at several other locations in Great Britain. Under the 1947 UK–USA Agreements, the U.S. and the United Kingdom—as well as Canada, Australia and New Zealand—routinely exchange information gleaned from intercepted telecommunications.

"For the purpose of this directive, the terms "Communications Intelligence" or "COMINT" shall be construed to mean technical and intelligence information derived from foreign communications by other than the intended recipients.

"COMINT activities shall be construed to mean those activities which produce COMINT by the interception and processing of foreign communications passed by radio, wire, or other electromagnetic means, with specific exception stated below, and by the processing of foreign encrypted communications, however transmitted. Interception comprises search, intercept, and direction finding. Processing comprises range estimation, transmitter operator identification, signal analysis, traffic analysis, cryptanalysis, decryption, study of plain test, the fusion of these processes, and the reporting of results.

"*COMINT and COMINT activities as defined herein shall not include (a) any intercept and processing of unencrypted written communications,* press and propaganda broadcasts, or (b) censorship." (emphasis added)

The NSA contends that the specific exclusion of unencrypted written communications, which would appear to prohibit its interception of telegrams, "is and always has been limited to mail and communications other than those sent electronically." [76] Hence, the NSA appears to have interpreted this directive as a carte blanche to intercept and process all foreign communiactions, i.e., all those in which at least one terminal is foreign, even though such communications were unencrypted."[77]

Operation SHAMROCK, the code name under which the cable companies made most of their international telecommunications traffic available to the NSA, and to a lesser extent to the FBI, was terminated by the Secretary of Defense in May 1975—a date coinciding with the Church Committee's first demonstration of interest in the program.

The "take" from Operation SHAMROCK, and from other NSA operations, was used by the NSA in the 1960's and early 1970's to compile files on American citizens. The NSA maintained a "watch-list" of names of individuals and organizations against which the "take" was sorted.

MINARET was the code name applied to the NSA's efforts to protect its watch-list on American citizens from disclosure. The watch-list had actually begun in the early sixties but the MINARET restrictions on disclosures were not applied until 1969.[78] The MINARET charter described the watch-list program as envolving "communications concerning individuals or organizations involved in civil disturbances, anti-war movements and demonstrations and military deserters involved in anti-war movements." [79]

MINARET was considered so sensitive that information being disseminated was classified Top Secret and labeled "Background Use Only," and while handled as SIGINT and distributed to SIGINT recipients,[80] it was specifically not identified as having any NSA connection.[81] [82] On May 12, 1976, material collected under the NSA watch-list program was transferred to the office of the Principal Deputy Assistant Secretary of Defense for Intelligence, Thomas K. Latimer, for safekeeping.[83] The MINARET files remain, as of March 1, 1977, in a safe in Mr. Latimer's office, retained pending a request for their production in a civil litigation.[84]

---

[76] Church Committee Final Report, Book III, p. 737.

[77] Former CIA Director Allen Dulles has defined communications intelligence as "information which has been gained through successful cryptanalysis of other people's traffic." He has defined cryptanalysis as certain codes and ciphers that can be the mathematical analysis of intercepted traffic. (Allen Dulles, "The Craft of Intelligence." Harper & Row, 1963; p. 73). Dulles' characterization of COMINT excludes the utilization of plain-text messages.

[78] Church Committee, Ob. cit., p. 739.

[79] "Establishment of Sensitive SIGINT Operation Project Minaret," dated July 1, 1969, in Church Committee Hearings, Vol. 5, pp. 149–50.

[80] SIGINT recipients include, but are not limited to, the President's Foreign Intelligence Advisory Board (PFIAB), the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), the Defense Intelligence Agency (DIA), the (Army) Assistant Chief of Staff for Intelligence (ACSI), the Office of Naval Intelligence (ONI), the Air Force Office of Special Investigations (AFOSI), the Energy Research and Development Agency (ERDA) and the Department of State's Office of Current Intelligence.

[81] Church Committee Hearings, Vol. 5, p. 150.

[82] For a detailed discussion of NSA watch-list activities, see Church Committee Hearings, Vol. 5, pp. 1–55 and 145–163; also Church Committee final Report, Book III, pp. 737–65.

[83] Letter from Comptroller General of the United States Elmer G. Staats to Chairwoman Bella S. Abzug, November 12, 1976, p. 2.

[84] House Gov. Ops. Subcommittee on Gov. Information and Individual Rights staff telephone interview with Col. Stephen A. Harrick, Office of Assistant Secretary of Defense for Legislative Affairs, March 1, 1977. (The civil litigation is *Halkin v. Helms*, 75–1773, U.S. District Court, District of Columbia Circuit.)

SHAMROCK

Pressure had been exerted on the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities. (Hereafter referred to as the Church Committee and cited as the "Church Committee Hearings" and "Church Committee Final Report".) On October 1, 1975, Attorney General Edward Levi personally asked Senator Church on behalf of the President to postpone committee hearings on selected National Security Agency activities, scheduled for October 8 and 9, at which NSA Director Lew Allen, Jr. was to testify. The Church Committee agreed to delay Gen. Allen's appearance indefinitely.

Prompted by a press report,[85] The House Subcommittee on Government Information and Individual Rights initiated in August, 1975, an investigation into the interception and monitoring, by federal intelligence agencies, of telegrams and other forms of data transmissions entering and leaving the United States. The investigation was undertaken pursuant to the Subcommittee's oversight responsibility for matters concerning the rights of privacy of American citizens and for the operations of the Federal Communications Commissions. Public hearings were held on October 23, 1975, and February 25, March 3, 10, and 11, 1976. These hearings were conducted in the face of intense Executive branch efforts to have them curtailed or postponed.[86]

Whereas the Church Committee had conducted its NSA investigation by going directly to that Agency, the House Subcommittee approached no government agency, going instead to the international telegraph companies who allegedly had participated in such activities. These companies were initially responsive. It was apparently not until October 21, 1975—two days prior to the House Subcommittee's initial hearing—that the Administration became aware of the House Subcommittee's investigation, at which time it reacted strongly. On that day, the House Subcommittee received a letter from FBI Director Clarence Kelley, advising that a former FBI special agent, with whom the subcommittee had been dealing directly, would not be allowed to testify.[87] On the same day, as a result of government pressure, the two largest international common carriers—RCA Global Communications and ITT World Communications—suddenly withdrew their offers to appear voluntarily and demanded that they be issued subpenas prior to testifying. (A representative of another communications carrier subsequently informed the subcommittee that highly placed Justice Department officials, immediately prior to the subcommittee's October 23rd hearings, urged the company to demand subpenas. The company did not accede to the Executive branch request.)

On October 22, the House Subcommittee Chairwoman, Representative Bella S. Abzug, was visited by Deputy Attorney General Harold Tyler, NSA Director Allen, Assistant Secretary of Defense for Intelligence Albert Hall, Special Counsel to the President Jonathan Marsh, and White House Congressional Liaison Charles Leppert, all of whom requested the hearings not be held on grounds of jeopardizing either a Justice Department criminal investigation or jeopardizing national security.

On October 23, moments before the House Subcommittee's hearing was to begin, Attorney General Levi, unannounced and uninvited, arrived at the hearing room to visit the Chairwoman, bearing essentially the same message. Like the previous visitors, Mr. Levi could neither say which "national security" interest were in jeopardy, nor suggest to the subcommittee any guidelines beyond postponement or cancellation. The House Subcommittee's hearings proceeded as scheduled, but former FBI special agent Joe R. Craig, and representatives of RCA Global Communications and ITT World Communications refused to testify unless subpoenaed. Testimony was taken from representatives of American Telephone and Telegraph Company and one of its operating subsidiaries, the Chesapeake & Potomac Telephone Company.

Within two hours of the close of the subcommittee's October 23 hearings, the Church Committee reversed its earlier decision and voted to hold public hearings on the NSA.

---

[85] Frank Van Riper, "Find U.S. Agents Spy on Embassies' Cables." New York Daily News, July 22, 1975, p. 2.

[86] House Government Operations Subcommittee on Government Information and Individual Rights, Hearings, Interception of Nonverbal Communications, Oct. 23, 1975; Feb. 25, Mar. 3, 10 and 11, 1976, pp. 2–3.

[87] Ibid., p. 62.

On October 29, NSA Director Allen, accompanied by NSA Deputy Director Benson Buffham and NSA General Counsel Roy Banner, appeared before the Church Committee in public session, essentially confining their testimony to the Agency's "watch-list activity," which primarily operated under the code name MINARET. A second matter scheduled to be taken up at the hearings, identified as Operation SHAMROCK was temporarily put off.

On November 6, Sen. Church read the committee's SHAMROCK report, a summary of the Church Committee's investigation of the NSA that was to be made public into the record.[88] No testimony, however, was elicited in public session.

The report primarily dealt with contacts between U.S. telegraph companies and government representatives between 1947[89] and 1975, and procedures by which private communications entrusted to the carriers were turned over to the NSA and, to a lesser extent, the FBI. The report did not discuss how the information made available to the intelligence agencies was utilized by its collectors, or to whom it was disseminated, or the uses made of it by those entities—subjects of vital interest to the House Government Operations Committee.

On February 4, 1976, the House Committee issued subpoenas ad testificandum and subpoenas duces tecum to three FBI special agents, one former FBI special agent, one NSA employee, and executives of ITT World Communications, RCA Global Communications, and Western Union International. On February 17, President Ford instructed Secretary of Defense Rumsfeld and Attorney General Levi "to decline to comply with the subpoenas" directed to the government and government witnesses, stating that disclosure of the records sought by the Committee was not in the public interest.[90] Immediately, Secretary Rumsfeld instructed the NSA employee, and Attorney General Levi instructed the one former and three current FBI employees, that the Committee's subpoenas duces tecum (due February 18) were not to be complied with, inasmuch as "President Ford has asserted executive privilege." [91] On February 17, Attorney General Levi also requested "that Western Union International honor [President Ford's] invocation of executive privilege, and that it not produce and deliver documents described by the said subpoenas." [92] These applications of "executive privilege" to private corporations and to former government employees, were unprecedented expansions of that concept.

On February 25, the aforementioned former FBI employee, three current FBI agents, and one NSA employee appeared before the subcommittee, but refused to testify. Both the present and former FBI agents refused to testify on instructions from the Attorney General, while the NSA employee refused on orders from the Deputy Secretary of Defense, William P. Clements, Jr. Because of their failure to give testimony, the House Subcommittee recommended that all five be cited, pursuant to 2 U.S.C. 192, for contempt of Congress. Four of the witnesses were also recommended for contempt citations for their failure to produce documents.

On March 3, the Executive Vice President of Western Union International testified before the subcommittee, and turned over an eight year old list of NSA targets, the production of which President Ford had attempted to block by asking the corporation to honor his claim of the application of "executive privilege."

Attorney General Levi also asked RCA Global Communications that their representatives neither testify before the subcommittee, nor produce documents, "until procedures can be agreed upon to assure that the President's invocation of executive privilege is not effectively undone." [93]

Without procedures being "agreed upon," representatives of RCA Global Communications did testify on March 3, as well as on March 10, and subsequently turned over to the subcommittee additional records that the company had previously considered as not covered by the House Subcommittee's subpoena duces tecum.[94] Also on March 10, the House Subcommittee received the testimony of the Chairman of the Federal Communications Commission, Richard E. Wiley.

On March 11, representatives of ITT World Communications, which did not receive an "executive privilege" request from Attorney General Levi, testified before the House Subcommittee.

---

[88] Church Committee Hearings, vol. 5, pp. 57–60.
[89] Subsequently amended to 1945.
[90] House Subcommittee Hearings, p. 56.
[91] *Ibid.*, pp. 58–59.
[92] *Ibid.*, p. 99.
[93] *Ibid.*, pp. 125–26.
[94] Ibid., p. 240, et seq.

Utilizing the telecommunications intercepted under Operation SHAMROCK, the NSA's Office of Security maintained approximately 75,000 files on American citizens between 1952 and 1974.[95] These files were apparently created from information obtained through SHAMROCK, and NSA's other intercept programs. Persons included in these files included civil rights leaders, antiwar activists, and Members of the Congress. For at least 13 years, CIA employees were given unrestricted access to these files, and one or more worked full time retrieving information that presumably was contributed to the CIA's Operation CHAOS, which existed from 1967 to 1974. It is not publicly known which component of the CIA the NSA's Office of Security files on American citizens were transferred prior to 1967, nor by what authority these transfers were made. The CIA's apparent receiving of information on American citizens on an established and regular basis, several years prior to the heretofore believed commencement date of that Agency's domestic surveillance activities is disturbing. According to the NSA, its Office of Security files on American citizens were destroyed in 1974.[96]

While there is no reason to believe that SHAMROCK continues today, wherein the NSA, or its representatives, is involved in hand-to-hand acquisition of international telecommunications, the Congress cannot report that the NSA no longer intercepts such messages by electronic means. Indeed, one can argue that if NSA were not, it would not be doing its job of intercepting foreign government telecommunications.[97] The NSA has—and has had for several years—the technical capability and resources to accomplish this task without the knowledge of complicity of the cable companies.[98] Thus, from the NSA's point of view, a program such as SHAMROCK is no longer an operational necessity.

LEGAL CONSIDERATIONS

The Fourth Amendment to the Constitution guarantees to the people the right to be "secure . . . in their papers . . . against unreasonable searches and seizures." It further provides that "no warrants shall issue, but upon probable cause."

The fact that NSA, and its predecessors, indiscriminately obtained without a warrant copies of virtually every international telegram leaving the United States would thus appear to violate this constitutional guarantee of privacy.

These intelligence activities would also appear to have violated section 605 of the Communications Act of 1934. That statute, enacted eleven years prior to the commencement of SHAMROCK, provided, in part:

"No person receiving, assisting in receiving, transmitting, assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect or meaning thereof, except through authorized channels of transmission or reception, . . .

"(6) on demand of other lawful authority . . ."

No court decision prior to the start of SHAMROCK has interpreted the phrase "on demand of other lawful authority" to mean anything other than some form of official process. In particular, no foreign intelligence agency had ever been designated by any court as "other lawful authorities" under this section, nor did the legislative history of the Act indicate that such an interpretation was intended.

The international telegraph companies which participated in SHAMROCK themselves did not interpret this "other lawful authority" exception in section 605 as legal justification for their participation. To the contrary, they informally attempted to have section 605 amended to permit, as a matter of law, the actions which they were being asked to take by the government. They agreed to participate, nonetheless, even in the absence of such a statutory exception, upon the assurances of the Attorney General and the President that they would not be prosecuted under the provisions of section 605. Whether these high-level assurances satisfied the legal requirement of section 605, i.e. constituted "demands of other lawful authority," has never been the subject of a judicial determination.

---

[95] For a detailed discussion of NSA Office of Security files on American citizens, see Church Committee Final Report, Book III, pp. 777–78.

[96] Church Committee Final Report, Book III, p. 778.

[97] This is not to argue for the continuation of SHAMROCK, or any SHAMROCK surrogate.

[98] See, for example, testimony of William Colby, "Central Intelligence Agency Exemption in the Privacy Act of 1974."

Section 605 remained in its original form until 1968, when it was amended to read:

"*Except as authorized by chapter 119, Title 18,* no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, or meaning thereof, except through authorized channels of transmission or reception . . ." (emphasis added).

The apparent purpose of this amendment was to allow communications companies to cooperate with federal agencies for purposes related solely to foreign intelligence collection, without fear of prosecution under section 605.

The 1968 amendment to section 605 did not specify which provision in chapter 119, Title 18 authorized private communications companies covered by the Act to cooperate with the foreign intelligence collection programs of the federal government. Section 2511(3) of Chapter 119 merely provides that "nothing contained in this chapter or in section 605 of the Communications Act of 1934 . . . shall limit the constitutional power of the President . . . to obtain foreign intelligence information deemed essential to the security of the United States . . ."

The Supreme Court, however, in interpreting this provision in the well-known *Keith* case, held that it "confers no power" and instead "merely provides that the Act shall not be interpreted to limit or disturb such power as the President may have under the Constitution."

The legal effect of 1968 amendment to section 605, therefore, remains unclear. It states that chapter 119 of Title 18 "authorizes" communications companies, and their employees—otherwise prohibited by section 605 from divulging the contents of telegrams in their possession—to divulge such information to the President for foreign intelligence purposes. The Supreme Court has ruled, however, that this "authorization" provision contained in section 2511(3) of chapter 119 is no "authorization" at all, but rather a recognition of the President's constitutional powers as head of state.

In any case, it would appear that even the 1968 amendment to section 605 would not permit communications companies from divluging the contents of telegrams to the government for other than foreign intelligence purposes. Yet such activity took place for several years after the 1968 amendment. Two of the participating telegraph companies made no distinction either before or after 1968 with respect to the nature of the materials turned over to NSA. NSA received copies of all messages, including those with no foreign intelligence value whatsoever. NSA, for its part, gleaned not only foreign intelligence information from such messages, but also information related to law enforcement and internal security matters. It would appear therefore that section 605, even as amended, was violated by those companies who furnished telegrams containing other than foreign intelligence information.

NSA PRACTICE

From a privacy standpoint, the problem of intercepting "foreign intelligence" telecommunications—regardless of whether NSA obtains them by wholesale company turnover of hard copy traffic or by more remote electronic means—is that in its effort to secure *all* foreign intelligence/national security messages of possible interest, the NSA is obliged to use a "vacuum cleaner" approach to intercept all messages and then filter out the messages it does not want, prior to distributing the messages it does want to its government consumers.[99] This philosophy is prompted by a combination of the government's desire to know "everything" that it considers to be "national security" related. This includes agricultural, cultural and social information, as well as military and political happenings, financial transfers, economic matters of both governmental and pro-

[99] Not even a single blanket "vacuum cleaner approach" satisfied the appetite of government monitors, for FBI and NSA "cable drop" operations in Washington partially duplicated and triplicated the New York Shamrock coverage. In these operations, the FBI physically entered the Washington offices of RCA Global Communications and ITT World Communications during daylight hours, to examine cable messages, and NSA repeated the operation between 3 and 5 a.m. (See House Government Ops. Hearings, p. 241; the Committee also was informally informed that the same persons who made nocturnal visits to RCA similarly visited the Washington offices of ITT.)

For sorting messages, the FBI paid RCA employees from 1960 to 1975; starting in 1966 the FBI began withholding 20 percent of these payments for income tax purposes. (Ibid, pp. 242–43; the Committee does not know if ITT employees received comparable message-sorting compensation from the FBI.)

prietary nature. Most telecommunications, whether they be individual, corporate, or governmental in nature, in fact travel over common circuits. This insures the NSA's access to all types of information. Indeed, former CIA Director William Colby claimed, in testimony given on August 6, 1975, "On some occasions, [the interception of U.S. citizens' telecommunications] cannot be separated from the traffic that is being monitored. It is technologically impossible to separate them." [100] In fact, Mr. Colby's use of the expression "on some occasions" is misleading inasmuch as the NSA ostensibly faces this problem in its search of international communication links entering and leaving this country.[101] Vice Adm. Bobby R. Inman is likewise faced with this same dilemma as he states that the NSA had made what he calls "inadvertent pickups" of the communications of United States citizens.[102]

Approximately 24,000,000 international telegrams and 50,000,000 telex messages enter, leave, and transit the U.S. annually.[103] The great majority of these messages are to and from U.S. persons.[104] Millions of additional messages are transmitted on leased lines. Computer data transmissions account for billions of words and numbers entering and leaving the country each year.

The NSA monitors this vast quantity of telecommunications by scanning these messages—as well as countless other overseas messages not entering or leaving the U.S.—as they are being transmitted by radio, microwave, and transmission cables. Such messages are then processed (in real time or at a later time) through computers that are programed to isolate encrypted messages, as well as messages containing "trigger" words, word combinations, entities, names, addresses, and combinations of addresses—as, for example, when addressee "X" and addressee "Y" are only conditional targets, that become activated by "X" communicating with "y", or vice versa.

The intercepted messages that are in code or cipher are, whenever possible, solved, and they, along with messages selected by "target procedures," are then inspected by human analysts.[105] Messages which the NSA electronically scans, and judges by certain programed criteria to be of no interest to NSA or its consumers for further screening and analysis—annually amounting to tens of millions of communications of U.S. citizens—are not considered by NSA to have been intercepted or acquired.

According to the Church Committee's report on the Shamrock program:

"Of all the messages made available to NSA each year, it is estimated that NSA in recent years selected about 150,000 messages a month for NSA analysts to review. Thousands of these messages in one form or another were distributed to other agencies in response to "foreign intelligence requirements." [106]

The "other agencies" that receive these messages "in one form or another" are those in SIGINT/COMINT channels. These agencies are also the essential suppliers of the "triggers"—the programed criteria—that activate target procedures. The usual (but not exclusive) form in which recipient agencies receive messages is in analytic reports prepared by the NSA, from excerpts of individual communications intercepts.

NSA representatives have repeatedly given Congress informal oral assurances that internal NSA directives exist to prevent the misuse of intercepted

---

[100] Pike Committee Hearings, p. 241.

[101] Mr. Colby's semantic qualifier, "on some occasions," is not unlike his testimony before the subcommittee and others, that the CIA's 20 year mail intercept program (which opened over 190,000 letters), was among "the few" individual instances of the Agency's domestic illegalities. Cf., for example, "Central Intelligence Agency Exemption in the Privacy Act of 1974" hearings, House Subcommittee on Government Information and Individual Rights, March 5, 1975 (p. 5) and June 25, 1975 (pp. 139–40).

[102] Hearings, Senate Subcommittee on Intelligence and Human Rights, 21 July 1977.

[103] Letter from R. Michael Senkowski, Legal Assistant to the Chairman, Federal Communications Commission, House Subcommittee on Government Information and Individual Rights, January 28, 1976.

[104] U.S. persons are U.S. citizens, resident aliens in the U.S. and corporations with their principal place of business in the U.S.

[105] These are headquarters procedures. Apparently, at overseas bases, many messages are also intercepted by human analysts prior to trigger word screening. Chet Filippo, an associate editor of Rolling Stone, reported that he was, in 1967, in the Naval Security Group (the NSA's naval wing), assigned to intercept telecommunications from a desert base in Sidi Yahia, Morocco. In addition to intercepting diplomatic cables, military messages, telegrams, transcripts of transatlantic phone calls, Filippo wrote, "I also screened reams and reams of transatlantic cables to and from the U.S., regardless of whether they contained any key words or names. Telegrams or phone calls involving American congressmen and journalists, 'dissidents,' multinational corporations—were all targets." (Chet Filippo, "Can the CIA Turn Students Into Spies?", Rolling Stone, March 11, 1976.).

[106] Church Committee Hearings, Vol. 5, p. 60.

telecommunications that are not "foreign-intelligence" related. Moreover, the former Director of the NSA, Lt. Gen. Lew Allen, Jr., has formally declared: "The executive directives applying to these efforts state: (a) The purpose of the signals intelligence activities of the National Security Agency is to obtain foreign intelligence from foreign communications or foreign electronic signals. (b) Foreign communications exclude communications between or among citizens or entities." [107]

Unfortunately, these statements shed little light on what the NSA actually does with the communications of American citizens which it might acquire. Furthermore, any related internal NSA guidelines of substance, no matter how tightly drawn they may be to prevent potential abuses, are so closely held that any violations will likely be undetected by Congress or any other authority outside the NSA. The only persons having access to these guidelines outside the NSA are a selected group within the Executive branch and a handful of "need to know" members and staff within the Congress, all of whose access to the information is based on the condition they will not disclose it. Moreover, briefings on high-priority or potentially embarrassing intelligence matters by federal intelligence agencies given to "need-to-know" individuals in Congress, are often vague and incomplete.[108] Furthermore, it is virtually impossible for any person or Agency outside the NSA to ascertain if the guidelines are, in practice, actually followed. The guidelines, therefore, being kept very secret, offer little assurance to the American people. Not only are they unknown, but no public evaluation of their effectiveness is presently permitted. In practice, the "system" is ultimately based on the rule of a very few men and not on the rule of law.

The Pike Committee's final report noted that "preliminary investigation reveals at least one new area of nonpolitical and nonmilitary emphasis in international intercept—economic intelligence. Communications interceptions in this area has rapidly developed since 1972, partly in reaction to the Arab oil embargo and the failure to obtain good information on Russian grain production and negotiations for the purchase with American corporations." [109]

If the NSA targets the telecommunications of governments of oil rich Middle Eastern countries, as appears likely, then presumably vast quantities of communications between these governments and the U.S. commercial entities are intercepted. The U.S. commercial entities themselves may not be target of NSA surveillance, but the effect is the same. This sort of indirect surveillance might, for example, be especially effective against U.S. banks, which serve as depositories for Arab oil countries. As of December 31, 1975, these countries had over $11 billion on deposit with the six largest U.S. banks—plus additional billions in other U.S. banks.[110] In fact, communications of such banks might conceivably be viewed by the NSA or the intelligence community as "foreign intelligence" since the precipitous withdrawal of these funds can readily be seen as a foreign policy weapon against the United States.

Indeed, a senior official of a giant U.S. multinational financial institution, which has well over $1 billion on deposit from a single Middle Eastern oil producing

---

[107] Letter from Lt. Gen. Lew Allen, Jr. to Chairman Otis Pike, House Select Committee on Intelligence, August 25, 1975; quoted in Committee's final report as published in Village Voice, February 16, 1976, p. 90.

[108] Until the formation of the Church Committee, these individuals were limited to selected staff members of the Armed Services committees in the Senate and the House, and the Defense subcommittees of the Appropriations committees in the Senate and the House. The House Government Operations Committee asked several of these staff members if, in the course of exercising their Committee's oversight functions, the NSA had ever briefed them on Operation SHAMROCK. Some of these individuals replied they were generally aware that the Agency from time to time inadvertently intercepted private sector communications; others said the first they knew of such activity was when they read it in the newspaper. The House Committee has received no indication that any of these individuals had a detailed knowledge of Operation SHAMROCK.

[109] Ob. cit., Village Voice, February 16, 1976, p. 88. (Emphasis added.)

[110] Attachment to letter from former Federal Reserve Chariman Arthur F. Burns to Sen. Frank Church, Chairman of the Subcommittee on Multinational Corporations of the Committee on Foreign Relations, March 9, 1976. The Federal Reserve refused to supply the Multinational Subcommittee with deposit totals of individual Middle East oil-producing nations, but the Washington Post noted that, in 1975, the government of Kuwait had $1.7 billion on deposit with the Citibank of New York, and in the same year foreign deposits accounted for nearly two-thirds of all monies deposited in both the Citibank and Chase Manhattan Bank, the nation's second and third largest banks. (Ronald Kessler, "Banks Hold Huge Foreign Deposits: U.S. Examiners Worried About Pressure From Governments," Washington Post, January 14, 1976, p. A-1.) By June 30, 1976, the deposits of the Middle East oil-exporting countries in U.S. banks reportedly totaled around $19 billion. (Dan Morgan, "Senators, Banks Block Probe of Arab Deposits," Washington Post, October 10, 1976, p. A-1.)

nation—as well as substantial deposits from several others—has advised the House Gov. Ops. Subcommittee on Gov. Information and Individual Rights that he has litle doubt the NSA is intercepting and analyzing his company's international telecommunications.[111] But this official, knowledgeable about the company's telecommunications "risk safeguard management," stresses that the company is not concerned about NSA intercepts, which it feels are legitimate. Rather, the company is only concerned with private interception, and it protects itself from this threat by encrypting its telecommunications at a level which makes it inaccessible to non-government third parties, but not inaccessible to the NSA. This corporate official also opined that his company, as well as most comparable businesses which use similar levels of encryption, had the resources and knowledge to encrypt their telecommuniactions so they would not be accessible to the NSA. The corporation has not made encryption level operationally higher because it would "run into a political morass with the Office of Munitions Control" in Washington, and "we do not feel threatened by government monitoring."[112]

Congress does not know the parameters of the commercial monitoring program, but it has received information which suggests it is very broad. In one case related to the House Government Operations Subcommittee on Government Information and Individual Rights, a U.S. businessman owning a small company was briefly engaged in the selling of commercial building products to a Middle Eastern oil sheikdom; the entire transaction was conducted by international telephone and telegram. Shortly after his first communication, he and his wife were interviewed by federal intelligence agents knowledgeable about the proposed sale. The couple was then kept under physical surveillance until shortly after the transaction was completed. In another case, members of a Washington law firm, involved in international trade, in litigation with the Department of Justice on behalf of a client, related to the Subcommittee that the government has used evidence which could only have been obtained from intercepted cable and telex messages. Regrettably, the firm feels it is not in its client's best interests to pursue the matter.

These allegations appear to partially conflict with information supplied the House Government Operations Subcommittee on Government Information and Individual Rights by the General Accounting Office (GAO), which, after reviewing NSA intelligence reports by employing sampling techniques, found "no unauthorized use of the names of U.S. Persons."[113]

But the GAO has neither defined nor characterized "unauthorized;" it has merely stated that the NSA "takes great pains to remove the identity of the U.S. person from any foreign intelligence report," and noted that in the course of making its random sampling of NSA intelligence reports, it "did find three instances in which the mention of equipment might identify the U.S. manufacturer to a knowledgeable person."[114] The report thus suggests that the NSA is intercepting, analyzing, and disseminating information obtained from the telecommunications of U.S. commercial entities—whether or not such entities are being identified by name, which suggests that the Pike Committee's observation that economic intelligence of a non-political and non-military nature is being intercepted is clearly accurate.

---

[111] Telephone interview, December 14, 1976.

[112] The Mutual Security Act of 1954, as amended, establishes controls on "the export and import of arms, ammunition, and implements of war, including technical data relating thereto, other than by a United States government agency." Category XIII, "Auxiliary Military Equipment:" subsection (b) includes:

"Speech scramblers, privacy devices, cryptographic devices (encoding and decoding), and specifically designed components therefor, ancillary equipment, and especially devised protective apparatus for such devices, components and equipment." (Source: International Traffic in Arms Regulations, Department of State; February 1976, p. 5.)

The Act is administered by the State Department's Office of Munitions Control, assisted by the Department of Defense, which grants (and withholds) export licenses. On November 23, 1976, the Secretary of Commerce signed a Data Encryption Standard developed by the National Bureau of Standards, assisted by the National Security Agency. Many critics of this standard maintain it is set at a level (56 binary digits, or "bits") which allows the NSA and, in time, very large corporations, to penetrate it. A November 18, 1976 Bell Laboratories memorandum characterizes the standard as having "little safety margin," and urges that it be strengthened to 64 or 128 bits. An official of the Office of Munitions Control has advised that for export use, "anything above 56 bits you have to come to us," adding that "one large U.S. corporation wants to use more bits in several overseas situations and in some cases we are going to grant permission." (Telephone interview with Mr. Cylde Bryant, January 5, 1977.)

[113] Letter from Comptroller General of the United States Elmer G. Staats to Chairwoman Bella S. Abzug, November 12, 1976, p. 5.

[114] Ibid, p. 5.

What is an "authorized" use of the NSA's intercept capabilities? It may be very broad. In December 1976, for example, the Washington Post reported that the CIA had, for years, been conducting—with the knowledge of President Ford and Attorney General Levi—electronic surveillance operations against Micronesians who were negotiating with U.S officials over the future status of their islands.[115] As such, the Micronesians were "authorized" CIA targets, notwithstanding Micronesia's being a United Nations trusteeship administered by the Interior Department. Presumably the NSA was similarly "authorized" to treat telecommunications within Micronesia, as well as between Micronesia and the continental U.S., as being "foreign communications" within "foreign intelligence criteria."

Another example of what might be considered "foreign intelligence" is suggested by the Executive branch's maintenance of up-to-date inventories of a myriad of raw materials, worldwide. One possible source for this information could be the contents of telecommunications of multinational corporations. Could the contents of these messages—with the identity of the U.S. corporation deleted from disseminated intelligence report—be considered as "foreign intelligence"?

Similar examples of what could be considered as "authorized" "foreign intelligence" targets are communications which reveal international financial transactions, and foreign commodity transactions.

The critical point of these presumptions is not so much their validity as the ease with which they *can* become true—if they are not already! As presently constituted, NSA procedures are established and maintained by the NSA and its SIGINT/COMINT "customers" under secret internal directives which make the intelligence community unaccountable to the Congress, and, on occasion, even the President.[116]

Another crucial area kept equally secret by the NSA, is the quantity and nature of intercepted telecommunications that it can actually read. Several knowledgeable sources have advised that the NSA, while able to collect virtually all telecommunications, as a practical matter is unable to read the sensitive traffic of developed nations. This results from advances in computer technology, which have enabled the codemakers to outstrip the codebreakers. This position has been publicly expressed by David Kahn:

"But cryptology has advanced in the last decade or so, to systems that, though not unbreakable in the absolute, are unbreakable in practice. They consist essentially of mathematical programs for computer-like cipher machines. They engender so many possibilities that, even given torrents of intercepts, and scores of computers to batter them with, cryptanalysts could not reach a solution for thousands of years. Moreover, the formulas are so constructed that even if the cryptanalyst has the ideal situation—the original plain text of one of the foreign cryptograms—he cannot recreate the formula by comparing the two and then use it to crack the next message that comes along.

"Electronic machines embodying these techniques replaced machines from World War II in the State Department shortly after the Cuban missile crisis. Other rich countries have also begun to use such devises. But poor countries still have not. Consequenty, the NSA can no longer solve the high-level messages of the major powers. It has earlouds of intercepts of them on sidings at its headquarters at Fort Meade, Md.—but only those of the third, and fourth-rate powers [are being deciphered]. Their messages, however, seldom provide insights into plans seriously affecting the United States." (New York Times, June 22, 1973)

If Kahn's assessment, along with that of others, is accurate, and there is little reason to doubt its validity,[117] the NSA is largely "out-of-business" *vis-a-vis* the understanding of the body of intercepted encrypted telegraphic foreign intel-

---

[115] Bob Woodward, "CIA Bugging Micronesian Negotiations," Washington Post, December 12, 1976, p. A–1.

[116] In 1970, when President Nixon endorsed the so-called Huston Plan, under which the NSA would intercept the private communications of American citizens, he was unaware that the NSA had for years been conducting a watchlist program similar to what he was proposing; there is no indication the NSA ever informed him of its watch-list activity.

[117] Kahn is highly esteemed. Lyman B. Kirkpatrick, Jr., former Inspector General of the CIA, has characterized Kahn's "The Codebreakers" as "the most authoritative book on communications intelligence" (in "The U.S. Intelligence Community: Foreign Policy and Domestic Activities," Hill & Wang, 1973; p. 198). William Stevenson, Winston Churchill's Chief of British Intelligence in World War II, has described Kahn's work as "indispensible to the serious student of cryptology" (in William Stevenson, "A Man Called Intrepid," Harcourt Brace Jovanovich, 1976; p. 344n).

ligence telecommunications traveling on circuits most often shared with U.S. citizens, into and out of the U.S.[118, 119, 120]

The National Security Agency has become so sensitive about the fact their primary raison d'être is evaporating that they are undertaking heroic measures to prevent the Administration in general and Congress in particular from understanding the true limitations of the code breaking ability. Such a revelation would likely suggest to Congress that the withdrawal of some of NSA's billions of dollars would be in the best interest of the country.

Computer scientists and mathematicians are being harassed and intimidated by the National Security Agency as lawful research into information theory in the private, academic realm is being undertaken. In fact, the NSA is reported to have threatened physical damage to and "extra-legal" action against U.S. industry in the manufacture of unclassified encryption equipment for sale to banks and other legitimate businesses.[121]

CONCLUSIONS

Activities of the National Security Agency become relevant to us all when they infringe upon the privacy of American citizens. As long as that Agency's activities remain essentially uncontrolled and cloaked in undue secrecy, Americans cannot be certain that their privacy is not being silently invaded.

It appears the NSA, despite its astounding technological capabilities, can no longer decipher most high-level messages of developed nations; that the comprehensible COMINT "take" consists of: (a) relatively low-level encrypted messages of developed countries; (b) telecommunications of relatively unsophisticated countries; and (c) plain-text telecommunications.

The technical capabilities of the NSA are such that they offer any entity in a position to use them—the President, the Department of Defense, or other COMINT recipients—a stepping stone to varying degrees of domestic tyranny. Former NSA Director Allen's frequent assertion, that his agency does not initiate policies but only follows orders received from the United States Intelligence Board [now the National Foreign Intelligence Board] and its members,[122] does not inspire confidence that the NSA's boundless power will not be amenable to further abuse.

Though the NSA's operation SHAMROCK represented an invasion of privacy of American citizens vastly greater than any known FBI or CIA mail intercept program, and though its watch list activities *vis-a-vis* American citizens were deemed by former Attorney General Elliot Richardson, to raise "a number of serious legal questions which have yet to be resolved," [123] the NSA continues to function under a mantle of secrecy. It has not explained, and presumably does intend to explain, itself to the American people. It simply asks the public to "trust us."

We should not believe that such trust is justified. It is regrettable that a shroud of secrecy, as tightly drawn as ever, continues to envelope all the activities of the NSA. It is further believed that even if the NSA did not pose a significant threat to the privacy of American citizens, and if it had not abused its powers in this regard, that much of the secrecy surrounding its operations is obsessive and unfounded. The fact that it does pose a significant threat to the privacy of American citizens, and has a record of violating it for more than thirty years, strengthens one's belief that the NSA should explain to the public what it does with our communications, and should become publicly accountable for its activities that affect Americans.

---

[118] Private communication with Herbert S. Bright, President, Computation Planning, Inc., Bethesda, Md. Bright, developer of commercially-available generalized support system for cryptographic privacy transformation of data, has challenged the NSA to break encryption methods developed by his company. Rather than suffer embarrassment and exposure to failure, the NSA declined this face-off.

[119] Scientific American, Mathematical Games, "A new kind of cipher that would take millions of years to break," Vol. 237, No. 2, August 1977.

[120] "Cryptography, On the Brink of Revolution?" Science Magazine, Vol. 197, 19 August 1977, p. 747.

[121] "Untold Story," Washington Merry-Go-Round, by Jack Anderson and Les Whitten, February 21, 1976.

[122] See for example, letter from Lt. Gen. Lew Allen, Jr., to Attorney General Elliot Richardson, October 4, 1973, in Church Committee Hearings, Vol. 5, pp. 162–63.

[123] Letter from Attorney General Elliot Richardson to Lt. Gen. Lew Allen, Jr., October 1, 1973, in Church Committee Hearings, Vol. 5, pp. 160–61.

Much of the basis for the NSA secrecy is historical habit, in which intelligence agencies traditionally attempt to keep everything—even, when possible, their very existence—hidden. This secrecy is often maintained even when foreign adversaries are admittedly familiar with many details of a particular operation.[124]

The NSA has vigorously fought other possible disclosures which will not endanger the national security. Though the NSA acknowledges that it monitors telecommunications of "foreign intelligence interest," and it is generally accepted in diplomatic and intelligence circles that the Agency monitors the telecommunications of most foreign governments, the NSA, strongly reinforced by the White House and the Defense and Justice Departments, considers it unthinkable, for example, to identify even by categories, countries in which it has an intelligence interest.[125] This attitude is maintained even though Herbert Yardley had, in 1931, listed 21 countries, including some of our closest allies, whose codes we were breaking 50 years ago, in peace time. Foreign governments today can hardly believe the NSA is currently doing any less, in view of the Cold War and the ease with which modern technology allows the NSA—and counterpart organizations of other governments—to acquire message traffic. Moreover, in 1972, in a long narrative, a former NSA analyst stated that "NSA monitors every government," and went on to give details of how the NSA monitors the traffic of several specific countries, including Great Britain, our closest ally.[126]

The monitoring of British traffic has been confirmed to the House Government Operations Subcommittee on Government Information and Individual Rights by a former employee of the Army Security Agency facility at the Vint Hill Farms telecommunications receiving station, 35 miles southwest of Washington, D.C. in the Virginia countryside. "We had a whole bank of machines," he relates, "I was

---

[124] Examples of this attitude are legendary. The government's reconnaissance satellite program, for instance, is managed and planned by the National Reconnaissance Office (NRO), an intelligence agency of the U.S. Government that is probably second only to NSA in budget expenditure. So secret is the NRO—which performs missions for the Department of Defense and the CIA—that instead of having an identifiable structure, its officials operate under the cover of other organizations. But the existence and functions of the NRO are undoubtedly better known to Soviet leaders than to American taxpayers, most of whom never heard of the NRO. (The detailed operations of the Soviet Union's counterpart to the NRO, which also as a worldwide reconnaissance satellite program, is similarly better known to U.S. intelligence officials than to Soviet citizens.)

The Washington Post has described the NRO as spending "an estimated $1.5 billion a year acquiring and managing the most sophisticated, elusive and expensive force of spies that has ever been recruited into the government's service." (Laurence Stern, "1.5 Billion Secret in Sky: U.S. Spy Unit Surfaces by Accident," Washington Post, December 9, 1973, p. A–1.) Two years later, the New York Times described the NRO as a semi-autonomous unit "under the Air Force that runs the satellite photograph program, set to spend under $2 billion." (Leslie Gelb, "U.S. Intelligence Cost is Put at $4 Billion," The New York Times, November 10, 1975, p. 40.)

Another case in point is the CIA's use of the Glomar Explorer to raise a sunken Soviet nuclear submarine from the floor of the Pacific Ocean: Soviet leaders knew of the CIA's effort, our government knew that they knew, and the Soviets knew that the U.S. government knew that they knew. Only the American (and Russian) people were uninformed. Similarly, in 1969, while the U.S. was surreptitiously bombing Cambodia with B–52's, the public was not told—though it was certainly no secret to the Cambodians, nor Soviet, Chinese, nor Vietnamese intelligence.

These incongruities often exist to hide embarrassments, often to hide illegalities or improprieties, often out of the "spy mentality" or the mentality that wishes to control information it would otherwise be obliged to share. In part, the NSA must be seen in this light. In its wish to avoid publicity, to avoid making public statements, it has—up until recent congressional investigations—attempted to function as if it did not intercept the telecommunications of foreign governments. Indeed, it has attempted to function as if it did not exist. The congressional investigations brought forth an NSA admission that could not have been a surprise to any foreign government, namely that the Agency does, in fact, intercept telecommunications of "foreign intelligence interest."

[125] So unthinkable is such disclosure that President Ford invoked "executive privilege" to apply to a private corporation, in an attempt to prevent the turnover of an old NSA list of countries whose telecommunications the Agency had expressed an interest in intercepting. The contents of this list had long been known to both the company's outside counsel and selected company employees. On October 22, 1975, NSA Director Allen was informally asked by a subcommittee staff member, "What security clearance does a company employee who transmits messages have?" Allen replied, "None." Apparently, in the view of NSA, these individuals are entitled to information that the Congress is not.

[126] Winslow Peck, "U.S. Electronic Espionage: A Memoir," Ramparts, August 1972. (Reporting on Peck's allegations, the New York Times stated: "Extensive independent checking in Washington with sources in and out of the Government who were familiar with intelligence matters has resulted in the corroboration of many of his revelations. But experts strongly deny that the United States has broken the sophisticated codes of the Soviet Union or other foreign powers." Benjamin Welles, "Ability to Break Soviet Codes Reported," New York Times, July 16, 1972, p. 1.)

one of a whole team of men whose only job was to read and process intercepted British communications." [127]

On a more mundane level, the NSA, in order to keep its activities secret, has interpreted the Privacy Act of 1974 [128] in a far more restrictive way than any other intelligence agency, including the CIA. That law requires, without exception, that each agency which maintains "systems of records" on individuals must publish notice of the existence and character of such systems. The CIA has accordingly listed, and described in some detail, 57 systems; [129] while much of the information contained therein is exempt from disclosure, that Agency has complied with the Act by explaining its systems—including those containing extremely sensitive information. But the NSA has responded to the Act by naming only 12 systems,[130] none of which relate to the NSA's operational activities. The systems the NSA has listed all relate to administrative matters, such as "Time, Attendance and Absence" of personnel, and "Equal Employment Opportunity Data," and initially these systems were not described in any way—except to say that they were exempt from disclosure. It was not until January 20, 1976, that the NSA publicly described these 12 systems, all of which remained relatively insignificant.[131]

The twelve filing systems reported by the NSA under the Freedom of Information Act do not contain reference to the kinds of files which information uncovered by the Church, Pike, and Government Operations Committees, would indicate are maintained by the NSA. There is, for instance, no record listed of there being a filing system of U.S. citizens whose communications were analyzed under NSA's Operation SHAMROCK for thirty years. Nor is there mention that the NSA supplied information on U.S. citizens to the CIA's Operation CHAOS, notwithstanding that such transfers have been frequently confirmed [132] and the Privacy Act states that each agency shall keep an accurate accounting of "the date, nature and purpose of each disclosure of a record (under its control) to any person or to another agency . . ."

On March 30, 1976, the House Government Operations Subcommittee on Government Information and Individual Rights requested, inter alia, that the Government Accounting Office "conduct a survey of all files and records stored or maintained by the National Security Agency to determine whether the agency has systems of records which might fall within the Privacy Act's coverage and which have not been listed in the notices published thus far." The subcommittee also requested that the GAO "examine the accounting logs maintained by NSA to see that they fulfill the accounting and disclosure requirements of the [Privacy] act." The GAO response of November 12, which concluded "That the Agency has substantially strengthened its policies and procednres, related to intercepted electronic communications, to insure that the operations of the Agency are conducted in such a way so as to provide proper safeguards to the rights and privacy of U.S. persons," did not speak to either of these segments of the subcommittee's request. This unresponsiveness is presumably because the GAO, according to its report, viewed "The detailed underlying our findings [as] highly classified and their disclosure would not materially alter [its] substance."

---

[127] Comparable intelligence activities against friendly countries have frequently been suggested, or specifically described, in published accounts. For example, Lyman B. Kirkpatrick, Jr., a former senior CIA official, has written: "No mission located on foreign soil can consider itself immune from audio surveillance," concurrently noting that "The insatiable maw of the intelligence community analyzed every communication of any conceivable interest, anxious to gain clues to information on the strengths or intensions of other nations." (The U.S. Intelligence Community, Hill and Wang, 1973; pp. 7–9.)

William Stevenson has written: "The most delicate field of cooperation (between Great Britain, Canada and the U.S., circa 1941) was communications intelligence, because it necessitated a disclosure of each country's apparatus for eavesdropping upon the coded radio traffic of other nations, an activity to which nobody wished to confess." ("A Man Called Intrepid," Harcourt Brace Jovanovich, p. 271.)

Francis Gary Powers has written that of all the information he withheld from the Russians, when captured in 1960, "the most dangerous, because of what the Russians could do with it," concerned the "special" U–2 flights that have the mission of spying on our own allies. (Francis Gary Powers with Curt Gentry, "Operation Overflight," Holt, Rinehart and Winston, 1970, p. 311.)

[128] 5 U.S.C. 552a, effective September 27, 1975.

[129] Federal Register, Vol. 40, No. 168, August 28, 1975, pp. 39777–801.

[130] Federal Register, Vol. 40, No. 166, August 26, 1975, pp. 37579–582; Federal Register, Vol. 40, No. 187, September 25, 1975, pp. 44294–297.

[131] Federal Register, Vol. 41, No. 13, January 20, 1976, pp. 3025–003.

[132] See, for example, House Subcommittee on Government Information and Individual Rights Hearings, "Central Intelligence Agency Exemption in the Privacy Act of 1974, 1975, p. 164; also, Church Committee Final Report, Book II, p. 101.

CLOSING REMARKS

Gentlemen, in the past few years we in America have turned a communications corner. It has generally become more expedient, more cost-effective, to send electronic communication, a phone call, a data transmission than to write a letter or send business tabulations by mail.

When our personal communications are being scanned in order to catch a few targeted "foreign agents," our privacy has been invaded. When our telegrams are dropped out for analysis simply because they contain the words Fidel, or U–235, or Vladavostok, or whatever, the Constitution has been violated.

When in the process of looking for spies and their activity we occasionally, inadvertently acquire the messages of non-targeted citizens, say less than one-half of one percent, I don't believe that any reasonably patriotic citizen would complain, especially if he is promptly notified of the fact.

When this "inadvertent" acquisition and scanning of our communications messages rises to several orders of magnitudes over actual targeted messages, then clearly minimization is not taking place; clearly a general warrant, a broad search and seizure is taking place.

Gentlemen, let me put this on a very personal basis. There are a few of us in this room who enlisted during World War II to fight aggression threatening the very existence of America, threats from without. Now, as then, I see a new threat, a threat from within, a threat as dangerous as then.

This new threat is coming about as several powerful interest groups claim special exemption from the Constitution on the strength of expediency—special privilege to acquire entry into the privacy of our communication.

To some, this may be a small thing, espeically when "national defense" is said to be involved.

I wish to suggest, however, that this issue of the privacy of our telecommunications; the keeping of them inviolate, or the broadband scanning of our messages under special provisions may lead to a new kind of republic, a new tyranny, unlike anything we have known in our two-hundred year history.

I wish to be quite blunt, a dramatic change in the quality of life in America is slowly coming about as a result of the gradual erosion of telecommunications privacy.

Your decisions on this vital issue, as S. 1566 is being marked-up, will be pivotal.

I strongly suggest that the shotgun word "targeting" be removed from the language of S. 1566 and that more precise terms such as "intercept" and "acquire" be used.

I suggest that broadband sweeping of telecommunications circuits be made altogether unlawful, and that, if criminal or national security wiretapping must be done at all, that it be done on the single, local subscriber telephone or telegraph line not on our microwave trunk circuits.

TESTIMONY OF MR. DAVID L. WATTERS, WASHINGTON REPRESENTATIVE, AMERICAN PRIVACY FOUNDATION

Mr. WATTERS. Thank you, Mr. Chairman.

Mr. Chairman, I would like to say a few words about microwave eavesdropping. A better title might be "Broadband Interception Practices and the Interception of Nonoral Communications."

This is an issue that has not received significant public airing before the committee. It is one which may set a terrifying constitutional precedent if not reasonably dealt with in S. 1566.

Senator Moynihan said that "yet a curious, even eerie, unwillingness exists to confront not merely the dimensions of the problem, but also to imagine that we in the United States can do anything about this."

I believe that we can do something about it. My purpose is to show that present laws are not providing the protection the American people need, under the Constitution, and that the proposed statute, S. 1566, is inadequate, and will continue to be inadequate even if all the suggestions of the civil libertarians concerning the strict definitions of "foreign agent" and "criminal standard" are maintained.

I hope to offer some constructive language to be used in S. 1566 and to suggest some reasons why this language should be adopted.

First let me say that I believe there is evidence to show that Operation SHAMROCK, to this date, continues to operate under another name and another technology. SHAMROCK, a broadband interception of sorts, you will recall, was that practice wherein the NSA and FBI were secretly and visually reading virtually every telegraph cable message entering or leaving the United States for the past 30 years. This practice was discontinued after discovery by this committee.

Now, however, there is reason to believe that the NSA is using the domestic and international communications long line systems, primarily the microwave networks, to accomplish the same examination of cables once attainable through SHAMROCK.

It appears that the positions taken by our intelligence community in general, and the National Security Agency in particular, regarding the use of broadband interception practices and the interception of nonoral communications, techniques which are particularly applicable to the microwave systems, are highly questionable in the terms of the Fourth Amendment to the Constitution forbidding general search and seizure.

By sweeping through our telecommunications systems, looking for trigger words, multifrequency address sequences, or peculiar data patterns, all part and parcel of our private messages, the National Security Agency is searching through the private effects of thousands of untargeted citizens in order to secure targeted objectives.

This is the same as if the FBI were to go down your street, house by house, enter your home, search through your private correspondence, and by reading only the outsides of envelopes and file folder tabs, would make judgments of whether there is a scintilla of doubt that you are a loyal American or that you are engaged in activity that they, for one reason or another, thought you ought not to be involved in. All of this searching would be done because someone on your street, under the remotest possibility, might be a foreign agent.

Not a person here would stand for such a physical search without the issuance of a judicial warrant on probable cause that you are involved in a crime. For some reason, however, there is less reluctance among us to allow electronic searches through our telecommunications if we just don't know about it.

Our intelligence agencies continue to this day to dance around the direct question of electronic surveillance on U.S. citizens. Pressed for further clarification of the stock phrase "no citizen is targeted," they respond with an equally stock retort that it is not possible to discuss this inasmuch as it deals with classified intelligence methods and techniques.

The clever use of the phrase "aquired by intentionally targeting that U.S. person" is perpetuated in S. 1566. The word is "targeted" not "intercepted."

The technology being employed identifies targeted trigger words in thousands of telegraphic or data messages, or identifies peculiar signals associated with phone calls as they pass through the dragnet. An automatic recorder then snatches out the whole message for later examination by agents. Thus, it is not "persons" who are the primary targets of these insidious kinds of surveillance; it is information which

is targeted. It is small consolation that the private communications of innocent citizens are being sucked up into the system.

Further evidence of the broadband sweeping of trunklines and microware beams is hidden among the S. 1566 amendments to title III, chapter 119, the current wiretap law. A stipulation is inserted which will permit warrantless wiretapping "for the sole purpose of determining the capability of equipment" when such "test period shall be limited to 90 days."

Let there be no misunderstanding here. There is only one category of wiretapping equipment or system which requires up to 90 days for test and adjustment, and that system is broadband electronic eavesdropping equipment, the vacuum cleaner approach to intelligence gathering, the general search of microwave trunklines. I make this assertion on the strength of over 25 years experience in the telecommunications profession. An ordinary, single line wiretap requires only 5 minutes to adjust and test.

Additional roots of the attempt in S. 1566 to achieve warrantless wiretapping through the clever use of language are traced through the stipulation of the first sentence of the act. Herein the definitions of the current wiretap law, chapter 119, are made to apply to the proposed statute in chapter 120. It is stated that "Except as otherwise provided in this section, the definitions of section 2510 of this title shall apply to this chapter."

The problem is found in the definition of intercept, stated to be "the aural acquisition of the contents of any wire or oral communication."

The inclusion of the word "aural" to the exclusion of any other kinds of acquisition has introduced confusion. By excluding nonoral communications from the wiretap law, the intelligence agencies have justified warrantless wiretapping of citizens for years. In fact, it could be reasonably argued that any citizen could engage in warrantless wiretapping of the nonoral variety with impunity.

It must be understood that the nonoral, nonaural proviso excludes digital telegraphic messages such as Telex, TWX, telegrams, cables, and other such similar data as missile telemetry, video television, facsimile, banking, business, credit, insurance, and medical information. It also excludes switching and signaling information used in the routing and billing of telephonic and telegraphic circuits.

Gentlemen, in the past few years we in America have turned a communications corner. It has generally become more expedient, more cost effective, to send electronic communications, a phone call, a data transmission than to write a letter or send business tabulations by mail.

When our personal communications are being scanned in order to catch a few targeted foreign agents, our privacy has been invaded. When our telegrams are dropped out for analysis simply because they contain the words Fidel or U-2 or Vladivostok or whatever, the Constitution has been violated.

When in the process of looking for spies and their activity, we occasionally, inadvertently acquire the messages of nontargeted citizens, say less than one-half of 1 percent, I don't believe that any reasonably patriotic citizen would complain, especially if he is promptly notified of the fact.

But, when this "inadvertent" acquisition and scanning of our communications messages rises to several orders of magnitude over the

actual targeted messages, then clearly minimization is not taking place; clearly a general warrant, a broad search and seizure is taking place.

Now, to some this may be a small thing, especially when national security is said to be involved.

I wish to suggest, however, that this wholesale invasion of the privacy of our telecommunications, the broadband scanning of our messages under special provisions may lead to a new kind of republic, a new tyranny, unlike anything we have ever known in our 200-year history.

I wish to be quite blunt, a dramatic change in the quality of life in America is slowly coming about as a result of the gradual erosion of telecommunications privacy. Your decisions on this vital issue, as S. 1566 is being marked up, will be pivotal.

I strongly suggest that the shotgun word "targeting" be removed from the language of S. 1566 and that more precise terms such as "intercept" and "acquire" be used.

I suggest that the broadband sweeping of telecommunications circuits be made altogether unlawful, and that if criminal or national security wiretapping must be done at all, that it be done on the single, local subscriber telephone or telegraph line, not on our microwave trunk lines.

Thank you, Mr. Chairman. I request that the balance of my testimony be entered into the record.

The CHAIRMAN. Mr. Watters, we appreciate your contribution this morning, and that of the members of the foundation. I think there is a good deal of merit in some of your points there.

I assume that you and the foundation are familiar with the state of the law as it is now. After hearing your testimony, I wonder whether there is any purpose for this bill at all.

Would you rather have no law?

Mr. WATTERS. I believe we need S. 1566. I believe present law is inadequate. As an example, the very first definition in the wiretap law itself defines "wire communications." I will call it to your attention. "Wire communication means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire and cable. . . ."

This definition also includes the stipulation that such communication is carried by a "communications common carrier." Some have interpreted the definition to exclude any communication which might be transmitted through electromagnetic radiation such as radio. It is a sloppy definition, but adequate. In reality, it includes any radio communication and microwave communication when such communication is provided by a communications common carrier.

You will note in the very first part of the definition it says when any such communication is "made in whole or in part." Now, the "in part" may be that part wherein the wire communication travels only 1 inch by wire and then 100 miles by radio, but because it has traveled 1 inch by wire, the whole must be included in the definition of wire communication. However, our intelligence community has, in many cases, secretly elected to exclude any communication that is traveling by electromagnetic radiation as being covered by the wiretap law. The present bill, S. 1566, which would eventually be chapter 120, refers

back to this definition in chapter 119. Again, I believe this is a sloppy definition and I believe it needs to be clarified. All communications which are transmitted through communications common carriers should be covered by the protection of both chapters.

The CHAIRMAN. We are trying to deal with this very sensitive area both in S. 1566 and the charters, and we have not had a chance to view the way in which the charters will handle this. I would like for the staff to provide Mr. Watters with a copy of this. It is going to be public tomorrow. And we will want to see whether there are similar imperfections or whether one might shore up the other, and I appreciate having your thoughts.

But apparently you are not at all satisfied with the minimization procedures. We have tried to deal with the inadvertent acquisition of knowledge, and we do use that word instead of "intercept" thinking that that would deal with the "aural" problem.

Mr. WATTERS. There is a problem here in the minimization. As you read the existing wiretap law, the main thrust of the word "minimization" has to do with the acquisition, not the retention minimization. However, most of the language that has come before the Senate Judiciary Committee and before this committee has dealt with the retention minimization, the expungement of records. I think we need to deal very seriously with acquisition minimization. We must set up some procedure, some criteria. The acquisition minimization procedure needs to be included in the law, itself, rather than left open to some nebulous type of criteria that happen to be invented on the spot by an intelligence or law enforcement agent.

The CHAIRMAN. Well, we will examine your critique point by point. I appreciate your coming here and making it for us.

Senator Huddleston?

Senator HUDDLESTON. I would just comment that Mr. Watters' testimony illustrates a dilemma of the sort that we are faced with. Technology has advanced faster than legislation. I guess it is really a faster process. It has just been in recent months that we have become aware of the state of the art in the field of microwave interception. As the chairman has pointed out, we did address that problem in the charters, and hopefully you will have an opportunity to review that; it would be interesting to have your comment on it.

Mr. WATTERS. Thank you.

The CHAIRMAN. Thank you both, gentlemen.

Mr. ROSENFELD. Mr. Chairman, if there is 1 more minute, there is one point I would like to mention, if there is a minute.

The CHAIRMAN. All right.

Mr. ROSENFELD. The Judiciary report mentions that they expect that this committee will be dealing more fully with the oversight provisions, maybe adding additional oversight provisions to the bill. We were very dismayed to see that S. 1566 has a more limited report by the Attorney General to Congress than S. 3197 did, and the reasons explained in the Judiciary Committee's report why some of the things were taken out don't go fully to why the report was cut down. We think that report was very essential and that there was no reason why it shouldn't include things like a summary of the reasons given by judges for turning down a warrant applications when they are turned down, especially if those are to be kept secret, as the bill now contemplates. And

statements with regard to the use of the emergency powers, for instance, the number of times it is used and the instances in which the Attorney General felt it necessary to use the emergency powers, things such as this we think go a long way to informing Congress how this legislation was working, and merely giving a report that shows the number of applications made during a year and the number that were granted and the number turned down we don't think is terribly informative.

So we would urge the committee, if it is going to be adding oversight provisions to the bill, to consider requiring the Attorney General's report to have those sections in it.

The CHAIRMAN. Thank you.

We have got some language which would require quarterly reports, as I recall, or including this information you were talking about. Maybe we will let you take a look at it and have your thoughts on it.

Senator Huddleston, do you have any questions?

Senator HUDDLESTON. No further questions.

The CHAIRMAN. Gentlemen, thank you very much. We appreciate your helping us.

We will adjourn our hearings.

[Whereupon, at 12 noon, the committee recessed subject to the call of the Chair.]

MARKUP HEARINGS ON S. 1566—FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

FRIDAY, FEBRUARY 24, 1978

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, D.C.

The committee met, pursuant to notice, at 11:07 a.m., in room 457, Russell Senate Office Building, Senator Birch Bayh (chairman of the committee) presiding.

Present: Senators Bayh (presiding), Huddleston, Case, and Garn.

Also present: William G. Miller, staff director; Audrey Hatry, chief clerk of the committee; and John Elliff, Michael Epstein and Ed Levine, professional staff members.

The CHAIRMAN. May we convene, please.

I think everybody here is aware that we have been awaiting a quorum, and in the process, refreshing our memories about what is contained in this legislation which is rather complicated and extremely significant to the well-being of the country.

I don't know whether we are going to get a quorum or not, gentlemen. May I suggest that pending the arrival of a quorum, we go through the amendments which the staff and some of us feel are necessary to perfect the bill, discuss those one at a time. If anybody else has an independent amendment that might not fall in that previous category, he is certainly free to offer it. Then we will discuss it and hopefully will get a quorum.

If we don't get a quorum, then I will ask the staff, if there are no objections, to find a time when we can get enough Senators here to report this bill out because our time expires on the 28th, and it will be necessary for us to get additional time.

I should point out by way of providing an explanation, that this day was supposed to be the day for final action and Wednesday was supposed to be the day for the initial markup session. Almost everybody in this room knows we were engaged on the floor on Wednesday.

So if there are no objections, then, shall we proceed on that format?

All right, the first amendment goes to page 3, lines 6 through 19.

AMENDMENT NO. 1—FOREIGN PERSON TARGETING STANDARD

This amendment clarifies the existing "officer or employee" standard and ensures that foreign visitors to the United States are treated the same way as U.S. persons, unless they act on behalf of certain foreign powers.

Page 3, lines 6–19, delete and substitute—

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

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

"(ii) acts for or on behalf of a foreign power which engages in clandestine intelligence activities harmful to the security of the United States, when

the circumstances of such person's presence in the United States make it reasonable to conclude 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."

I point out that this part of the definition only applies to persons who are not U.S. citizens, that is, not U.S. citizens or permanent resident aliens. There are two separate paragraphs. Paragraph (i) deals with officers or employees of a foreign power. As reported by the Judiciary Committee, this paragraph reads, and I will quote, if you will look there, "is an officer or an employee of a foreign power." The problem with this is it includes anyone who is employed by his government in his home country and visits the United States in a purely private capacity. In other words, someone who may be a school teacher is a public employee in France who visits his long lost second cousin in the United States. That is really not the kind of person that we intend to cover under the bill.

Therefore, the amendment substitutes the words "acts in the United States as an officer or employee of a foreign power." This excludes the foreign tourist who just happens to be employed by his government at home, and I think that is really what we had in mind.

Paragraph (ii) if you will look to that in the amendment, is the standard for surveillance of a foreign visitor or visitors who are not acting as officers or employees of a foreign power in this country. Under S. 3197, the earlier version of this bill reported by the committee in 1976, as you recall, such foreign visitor was covered under the same standard that applied to the U.S. person. However, S. 1566, as proposed by the administration and reported by the Judiciary Committee, sets a lower standard for all foreign visitors to the United States. This lower standard is broader than necessary to deal with the FBI's foreign counterintelligence requirements. It seems to me we have a responsibility to make exceptions only when a good case has been made, and we have worked with the FBI and the Justice Department to develop the new standard, and it is tailored directly to the FBI's requirements.

We might just take 1 minute to define that. First of all, the person must be acting for or on behalf of a foreign power which engages in clandestine intelligence activities harmful to the security of the United States. Persons acting for such foreign powers are covered in two situations.

They are covered when the circumstances of their presence in the United States indicate that they may engage in such activities, that is, harmful clandestine intelligence activities, in the United States, where past experience of our intelligence agencies shows that certain classes of people have a significant degree of probability or possibility of being involved in the kind of activity that concerns us.

To pick one example that I think can be used without violating anything secure, past experience has shown that middle aged students in this country from the Soviet Union who have as their background a high degree of technical skills have in the past had more than the normal incidence of intelligence connections with the Soviet Union. It is that kind of person that we are trying to zero in on.

The FBI may know from this experience that a particular foreign power uses certain classes of visitors or a certain class of visitors to

carry out secret intelligence assignments. If the visitor falls in this particular class, it is not necessary to show that he actually has an intelligence assignment, but at least to watch and see.

Visitors acting for such foreign powers are also covered when they knowingly—I emphasize knowingly—aid or abet a person in the conduct of harmful clandestine intelligence activities, or when they conspire with such person knowing that such person is engaged in such activities.

Now, there are three relatively minor changes which I would like to ask unanimous consent to include in the text of the amendment that is before you. We are talking about (ii), if you look at the second line, I would like to strike out "harmful" and include "contrary" and strike out on the following line "security" and include "interests." And then on the fourth line, strike out "it make it reasonable to conclude" and insert "indicates." "Indicates" would be proper.

Now, that is where we are on that one, gentlemen.

It is open for debate and discussion. I would like to point out for the information of all the committee as well as interested citizens who are here that the stage where we are in this bill has involved probably the most intense negotiations between a number of groups and individuals who have a reason to be interested in this kind of legislation that I have experienced in my 16 years in the U.S. Senate.

I want to compliment the staff for their tenacity and their patience. I think if we are going to be successful, which we will be, we must be, we have to recognize that none of us certainly are—and I assume I speak for the other members of the committee as well as interested individuals and groups—none of us are going to be 100 percent happy with what we have, and yet I think it is important for us to keep our eye on this goal of getting legislation enacted such as this for the first time.

And having said that, I yield to my colleagues.

Senator GARN. I have no questions or problems with the amendment.

The CHAIRMAN. Is there further discussion on the first amendment?

Senator CASE. Excuse me.

The CHAIRMAN. Do you have further discussion on the first amendment?

Senator CASE. I just want to make exactly sure who is making the suggestions and why. The one you read is the State Department proposal?

Mr. MILLER. Justice.

The CHAIRMAN. It is Justice Department.

Senator CASE. Justice Department. In any event it was discussed with the Agency.

I just want to get some idea.

The CHAIRMAN. I can't speak for the Justice Department, but I am sure if the Justice Department were writing it, it wouldn't contain some of the strictures that are in it. I mean, it is the product of some significant negotiation. If we check with Mr. Epstein, Senator Hathaway's staff, who had the greatest interest in this particular matter, he seems to feel that that is within the bounds of our goals there.

Senator CASE. You mean the change from "security" to "interests" and so forth?

The CHAIRMAN. Yes.

Senator CASE. They are important changes.

I wonder if they would like to give us any relevant reasons why they are offered.

The CHAIRMAN. Well, frankly, they provide a little more leeway into, I think I can accurately describe this as lessening the protections a little bit, giving our governmental agencies a bit more opportunity to look at what is going on.

I have been very jealous or zealous, in my pursuit of this bill, to do that only when it looked like there was a reason. We are talking here, I would be quick to point out, about foreign nationals, not about American citizens. Additionally, in our history, our Constitution says that foreign nationals should be treated differently from U.S. citizens only where there is a reason.

The FBI and the Justice Department have convinced at least me that this is a particular area where you are talking about a certain class of people with a propensity to do the kind of damage that none of us wants to have happen or occur, but there is a reason, and that is why I am prepared to support that.

In the final analysis, the judge determines probable cause to see whether the individual involved is the kind of individual to which any of this would apply.

Senator CASE. This is, as you suggest, a broadening of the area which the government has.

Mr. EPSTEIN. But the amendment itself was intended as a tightening originally.

Senator CASE. You mean the committee proposal.

Mr. EPSTEIN. As the bill in this particular section was reported out by the Judiciary Committee, as I understand it, it would have permitted the targeting of a foreign official who was in this country engaged in clandestine intelligence activities, undefined, a visiting foreign dignitary, which would have permitted, even if he was acting in his official capacity, the targeting of a visiting official from a foreign country which was a friendly country and was only here engaged in lobbying, because clandestine intelligence activities are undefined.

So the original alteration of that particular frame of use defines clandestine intelligence activities which are harmful to the security of the United States, to make it clear that we were not just targeting foreign friendly officials who were visiting.

There was concern expressed by the Justice Department as to whether or not the use of the phrase "harmful to the security of the United States" might require them to prove almost a specific case of harmful act that was conducted against the United States, and they requested that the "harmful to the security" be modified to what the present language is, "contrary to the interest."

Senator CASE. But is it necessary in order to accomplish some added flexibility along those lines to suggest the concern you have, to change the noun? Can you not change the degree to which this activity is likely to have this result by saying "is or may be," something of that kind, rather than changing it from "security" to "interests" because "interests" is as wide as, you know—I don't know what you say, it is a great canopy almost.

Mr. EPSTEIN. The phrase itself doesn't go to the activity that the official engages in. It relates to the activities that that country is en-

gaged in, so we are really talking about hostile countries taking action contrary.

Senator CASE. The interests may be economic and may involve trade, could even involve cultural matters.

The CHAIRMAN. How could that be, my colleague, if we are talking about something that is harmful to the United States?

Senator CASE. Harmful to its interests, not to the United States, but to its interests. I mean, it is just such a broad word, and you could keep "security."

Mr. EPSTEIN. Contrary to the security interests?

Senator GARN. Well, let me say, if I might, that you are correct when you say it tightens and then loosens the tightening.

I think you need to recognize first of all the new definition. It excludes someone, whether they are a school teacher or whatever, that works for a foreign government, excludes them off the top from those categories, the casual foreign tourist that is coming through that has some government connection but is not working for or on behalf of them. I think it is actually necessary that we tighten that because this is an obvious invitation for the Soviets or anyone else to then, if we exclude them to begin with, to start using that kind of persons, say, well, as long as you are over there, check on this for us, do that.

So then, (ii), I think, becomes necessary to define it, OK, you exclude them to begin with but if it is found out that they are engaging in some of these things, then you can. I don't see it as great a loosening for our intelligence agencies as it might appear because off the top you have said you can't touch those people to begin with unless they meet these clandestine standards, unless once they get here they start doing something.

The CHAIRMAN. Here again, the judge is the one that makes this final determination. Perhaps we could put in the report language the kinds of concerns that we all have, to keep this interest as close to the judicial areas that we are concerned about as we possibly can.

I understand that the FBI is concerned that since they must go to the judge—and we are talking about foreign persons when we are establishing this requirement for the first time—since they must go to the judge to get this authorization, they are concerned that if you talk about "harmful to the security of the United States" you must be able to show specific kinds of harm from individuals who historically have been a class of people who more often than not have been involved in national security problems, but since you can't prove that about those individuals, you are not going to be able to sustain your request.

I should point out what Mr. Elliff has just reminded me, that the thrust of this whole amendment is a tightening thrust. The couple or three words we are talking about are stepping back, but the original draft amendment was just to let the clandestine intelligence activity stand on its own.

Senator GARN. The overall effect is still a tightening. To make sure I understand it, let me try it once more.

First of all, we are talking about a country whose interests or whose activities are harmful, but that doesn't mean that you can automatically target that person because of that. Then you have got to go to the second part, go to the court, the whole thing, so despite the fact that we are trying, by changing "harmful to the security" to "contrary

to the interests," that person cannot be targeted unless you have got the information in the second category here to go to the judge and get the warrant. So it is not really fair to say, at least in my opinion, that it is a loosening. It is an overall tightening. It is quite a bit tighter than the original bill, but it loosens the tightening just a tiny bit, but that person is still protected by the warrant procedures; is that correct?

The CHAIRMAN. Why don't we go on, unless there is further discussion, and everyone will have a chance in their own mind to resolve where they want to come down on this.

The second amendment amends the second part of the definition of "agent of a foreign power" on page 3 at line 20. It follows where we have been, on to page 4 on line 23, about all the next page, and this part of the definition applies to any person including a U.S. person, and the main purpose of the amendment is to establish a criminal standard for surveillance of U.S. persons.

AMENDMENT NO. 2—U.S. PERSON TARGETING STANDARD

This amendment provides a criminal standard for surveillance of U.S. persons. The standard is more flexible for spying (i) and for sabotage or terrorism (iii), than for other more nebulous clandestine intelligence activities (ii).

Page 3, line 20—page 4, line 23, delete and substitute—

"(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 the furtherance thereof, for or on behalf of a foreign power.

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

In my judgment, this amendment perhaps more than any other, has been the product of very intense negotiations and probably has resulted—well, I think we can strike "probably" and can say has resulted in at least a tentative agreement on a standard which resolves the most significant concern a lot of people had about the abuse of individual liberties.

There are four separate paragraphs as you note there. Paragraph (i) deals with spying. It covers any person who 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. Criminal statutes, violation of criminal statutes of the United States, that is the key phrase there, The words "may involve" make the standard more comparable to "reasonable suspicion" than ordinary probable cause. However, this is an improvement over the previous noncriminal standard which is paragraph (iii) of the bill as reported by the Judiciary Committee.

Here again, there are those of us who would have perhaps preferred a little stricter standard here than we have now. This activity is tied

with activities which will involve or may involve a violation of the criminal statutes of the United States.

Paragraph (ii) deals with a more nebulous area, "any other clandestine intelligence activities." This is basically covert political action by foreign intelligence services. The term is so vague, however, that it could border on political activities protected by the First Amendment. Therefore, the standard is stricter than for "spying" in two respects. First, the person must act pursuant to the direction of an intelligence service or network of a foreign power. Second, the activities must involve or be about to involve a Federal crime. Here again, nebulous as we recognize it is, we still tie that in with the criminal standard.

These safeguards, in my judgment, are needed to protect persons who are primarily exercising their First Amendment rights.

I understand that the Senator from Delaware will have an amendment which, as far as I am concerned, the committee should accept, which will tie this down even more specifically as far as protecting individual Americans in the full use of their political activities, the rights to be involved in and engage in political activity.

Why don't I go through (iii) because I understand from a drafting standpoint, the Biden amendment, which I recommend to all of you, will come at the end.

Paragraph (iii) now, I say to my colleagues, this negotiation has gone right on to the witching hour. We just looked at a couple of words that were proposed after we got into the room, and this process went on into the evening last evening. Paragraph (iii) deals with sabotage and terrorism, and this provision has turned out to be the hardest to draft. As proposed by the administration and reported by the Judiciary Committee, the standard is "knowingly engages in activities that involve or will involve sabotage or terrorism for or on behalf of a foreign power." The problem with this standard is that the words "will involve" require a high degree of certainty that terrorism will take place, especially when compared to the "may involve" standard for spying. Therefore we have tried to draft a standard that is more realistic.

The language of the proposed amendment reads "knowingly engages in sabotage or terrorism, or activities which are or may be in furtherance thereof, for or on behalf of a foreign power."

This standard, frankly, is not very satisfactory, because it is not very clear what activities "may be in furtherance of" terrorism. An alternative would be "activities which are or may be in preparation" for terrorism. The term "preparation" is more concrete than furtherance. It does not require evidence of preparation for a specific terrorist act, because the definition of "terrorism" speaks of "violent acts" and means a range of acts, not just one specific act. That goes to the definition of "terrorism."

I have asked the staff to research the law, and they advise me that "furtherance" has a very broad meaning, broader than I think we are really after here, and it is anything at all that makes terrorism more likely. On the other hand, "preparation" normally means preparation for a specific crime, which is too strict in this field.

However, the term "preparation" would not have its normal meaning because of the special definition of "terrorism." It could reason-

ably be interpreted to cover, for example, providing the means for the commission of acts of terrorism rather than one particular bombing.

Therefore, on the basis of this analysis, it may be better to change the amendment by deleting "furtherance thereof" and substituting "preparation therefor."

[Pause.]

The CHAIRMAN. So, just for the sake of having something to consider here, I am going to suggest that we put in "preparation," "activities which are or may be in preparation of terrorism."

I would be quick to point out for those who are concerned about "furtherance" that "preparation" is more strict, but for those who are concerned from a law enforcement standpoint that "preparation" is too strict, that you have to deal with one specific act, we are talking about "may be in preparation for" and we also go to the definition of terrorism, which is broader than one act. It encompasses a pattern or a plan, and for that reason I do not believe that it necessarily ties the hands of the law enforcement agencies to get these characters and put them where they ought to be put.

Senator CASE. Mr. Chairman, is there not something to the point an astute observer has made, that when you say "may," you also include "may not," and isn't that a pretty slippery word?

The CHAIRMAN. You are right, but you see, the whole problem here, we have been talking about somebody that may be passing some information. The immediate impact of that information is not going to be felt, so you have a little more time to deal with it and to prove the case. But if you are talking about somebody who is getting ready to blow up the Federal building or to take over an airplane and destroy it, we are talking about serious damage and lives. It seems to me we want to give a little more flexibility and that the difference is whether we are talking about before the fact or after the fact. I struggle with it, but it seems to me I come down on the side that the broader standard is permissible under these circumstances because it is better to give a little more leeway so you can keep this kind of an act from happening. What the Senator from New Jersey says is true, but as slippery as that little word "may" may be, I am prepared to go with it under the circumstances.

Senator GARN. Mr. Chairman, let me add to what you have said. I am not going to go back into the examples, but you have got to have more flexibility when you are dealing with this. I don't want to ever be in a position that I have tightened down something so much that—and I have protected somebody's free speech and have 150 people killed to protect that person's free speech. We are talking about terrorism and sabotage, and I can give you all kinds of examples where I think we can prevent things from happening, as I say, terrorist activities, because we knew about it in the past.

So although it is a slippery word, I think a slippery word is necessary in this particular case.

And something else I would like to remind my colleagues and everyone else about, regardless of what we talk about in these standards, ultimately to get a warrant, you have got to go to one of these seven judges. We have got to put some trust in those judges because right now that does not happen at all. If foreign intelligence is involved, any administration can order that bugging. So we are tightened down

considerably by having a warrant procedure, limiting the seven judges, and all the protection. And it has been a long time since we discussed this, and I just wanted to bring that out again. We are establishing some very strict warrant procedures, stricter, in many cases, than our present domestic situation because we are limiting seven judges where they can't go judge shopping. The limitations on length are very strict. So whether we have "may" in there or not, they still have got to go to a judge and convince him that these individuals should be tapped.

Senator CASE. Mr. Chairman, I don't disagree with anything you and Senator Garn and anybody else may have said on this. What it points up is in this area, this whole business of constitutional rights, there are no absolute rules, and I wonder sometimes whether we do a disservice, thinking that there are absolute rules. Everything depends upon the circumstances. That is not—maybe it isn't a good idea to say this very often, but it is true. We are not going to allow, whether you do what Mr. Lincoln said and Senator Garn was suggesting, we are not going to allow an innocent boy to be hanged in order to protect the constitutional rights of some scoundrel out in Kansas to agitate, put that guy in jail, and he did.

No, really, what the Constitution does here, and the Civil Liberties Union support is doing for us is keeping needling us to be aware of the dangers, and I agree with you basically. There is no possible way that you can write absolute rules in this, and I think it would be just as well for us to keep that in mind always and indicate degrees of severity, danger, concern, and just—at least, this is what I am going to have to try, that there will always be a time when the police chief or somebody else is going to go in, where it was in that book by somebody or other about a bird in the south that landed in this country. You wink at a guy who shoots at somebody who is just about to do a dastardly act. If this were not our attitude, then civil liberties would be in danger all the time from dictators.

That's all I want to say.

The CHAIRMAN. Well, we appreciate the Senator from New Jersey——

Senator CASE. Well, it is a trite thing, maybe, and it is so obvious that it isn't said very often, but I think it ought to be said because you cannot make these things as specific as we pretend we are making them.

The CHAIRMAN. I share his concern. I think we are all aware of the fact that what we are trying to do in this bill as well as the efforts that we have put in so far, and particularly the Senator from Kentucky, in the charters, is not only for these protections, but perhaps equally important, to have the oversight function of our committee, of the internal working mechanisms of the Justice Department, and of the judge who hands down these orders in the first place.

Now, you know, here we are, it is sort of like a high wire act over Niagara Falls, and I see very concerned and dedicated people sitting in this room who cringe at some of the words here, different words, I mean, you have those who are deeply concerned about civil liberties and are concerned about "may" and I am sure they are also concerned about the "preparation." They were concerned about "furtherance." Well, we changed that to "preparation" and then those who have the

responsibility for conducting our law enforcement mechanisms are concerned about that.

I think we have come as close here as we can to melding not the different interests, but the different legitimate concerns. I think the last thing this committee ought to do is to try to weigh this to see how we can dampen down the pressure on this side and weigh it off against the pressure on this side. I mean, we are not really in the business of trying to be popular. I mean, this provision, I think, is a good example of the responsibility and we end up making neither one of these groups happy, but I think we can take their experiences, their legitimate concerns, and we look at them and we sort of know, putting them together, that we have got to place as strong a provision in this area as we are ever going to get, and it is strong where we are right now.

Senator CASE. I agree, and it isn't a bad idea to recognize the kind of thing we are engaged in.

The CHAIRMAN. I think that is important to keep us on the mark.

Now, we did not deal with subsection (iv) there, which improves the aiding or abetting and conspiracy standard of the bill, as reported by the Judiciary Committee, by making clear that the person must "knowingly aid or abet any person in the conduct of activities" described in the first three paragraphs.

All right, I want to make certain of the first part of that, that is "knowingly aid or abet," but I think perhaps even more significant is that he also has to know the kind of activities that the individual is involved in so that you don't have somebody blindsided as a good Samaritan who doesn't really know what is going on.

[Pause.]

The CHAIRMAN. All right, before I yield to my patient colleagues, I think we should look at the amendment I referred to a moment ago that is recommended by our distinguished colleague from Delaware, Senator Biden, who has other important business and could not be here right now.

He has asked me to offer in his behalf an amendment to the definition of "agent of a foreign power" which I think is important. I would advise that the Administration is not opposed to this amendment. It would appear at the end of the "agent of a foreign power" definition there on line 23, on page 4, and it reads as follows. Now, I will read it and then I will ask the staff to get a printed copy, because this has been revised in the last hour.

Senator CASE. Beyond this?

The CHAIRMAN. Let me read it and it is in the process of being typed up right now, and I hope to get it to you in the course of the meeting. We didn't have a chance to study it before and make a final decision.

The amendment would read:

Provided, That no United States person may be considered an agent of a foreign power solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

I think that pretty well speaks for itself. Senator Biden, in his words, describes the need for it this way:

This amendment merely clarifies a point that has been raised on several occasions by critics of the bill that it should be clear in the legislation that the political activities of individuals in and of themselves should not be subject to electronic surveillance. In other words, the individuals should only be subject to surveillance under this bill based on conduct which threatens the national security or peace and tranquility, but not on mere speech or association.

It does not say that all kinds of political activity are protected. It does not say that just because you are involved in political activity you are safe. But if you are solely involved in political activity without other kinds of harmful activity, you may not be subject to electronic surveillance.

Now I yield.

Senator CASE. I think I like the language of the thing itself more than the explanation.

The CHAIRMAN. Perhaps it is the explainer.

Senator CASE. Well, I mean the explanation that we got on the previous draft of this amendment. There may well be speech that is harmful. It may be speech that, to use the old explanation of shouting fire in the middle of a crowded theater, and the incitation of a mob to racial violence is more than just speech in my opinion.

The CHAIRMAN. A fellow could be a citizen, could be my constituent, could be lobbying us to assume a certain position on the sale of arms, which it seems to me would be a legitimate position that a constituent, but if that constituent were operating under the direction of a foreign power, in addition to participating in the political activity—I don't want to use an extreme, but also helping to see that weapon systems plans or nuclear material was diverted contrary to law, the fact that he was engaged in political activity on the one hand would not protect him on the other.

Senator CASE. But I mean some things that are just speech could be violated. You can imagine, as I said.

The CHAIRMAN. They are not protected by the First Amendment.

Senator CASE. That's right, and that is why I like the amendment and I don't want the embroidery.

Senator HUDDLESTON. You mean like a Nazi political rally in a Jewish community.

Senator CASE. Well, as long as we leave it just with the language of the Constitution.

Senator HUDDLESTON. What if the person making such a speech makes a threat, says that we are going to blow up South Miami tonight at 7 o'clock or says that we did blow up South Miami last night at 7 o'clock. Is he protected under his speech clause that prevents any surveillance?

The CHAIRMAN. You get to the clear and present danger and probable cause there, which is different from case to case.

Senator HUDDLESTON. It would be incumbent to find some corroborating evidence.

The CHAIRMAN. Corroborating evidence or conduct that would lead one to believe that that statement is more than just puffery.

Senator HUDDLESTON. In the presentation of the report to the judge, could that be used as evidence, as part of a pattern of activities?

The CHAIRMAN. Yes, yes.

Senator HUDDLESTON. The fact that he made these threats, he made these plans.

The CHAIRMAN. Yes.

Is there further discussion on two?

Turn, if you will, to three. May I ask that we turn to four, please, and may I ask that we turn to five while the staff makes revision that involve only two words that are significantly different. And I will take the blame for them, but I would like to make sure that they are discussed.

AMENDMENT No. 5

This amendment provides that groups substantially composed of U.S. citizens or resident aliens shall have the same protections as U.S. persons, even if they are alleged to be covertly directed and controlled by a foreign government under part (F) of the "foreign power" definition.

Page 10, line 6, add after "powers"—"as defined in section 2521(b)(1)(A)–(E)."

Five amends the definition of "United States person," which now includes corporations or associations having a substantial number of members who are U.S. citizens or permanent resident aliens, unless such corporation or association is a "foreign power".

There is a problem with this exception because it means that groups which are substantially composed of U.S. citizens or resident aliens do not have the same protections as U.S. persons if they are alleged to be covertly directed and controlled by a foreign government under part F of the "foreign power" definition.

If you look at part F of the "foreign power" definition that includes any entity that is directed and controlled by a foreign power, even if the entity is substantially composed of Americans. There is concern that this might be used as a way to bypass the criminal standard for surveillance of individual Americans, by tapping instead the group that they belong to.

However, if such entities are substantially composed of Americans are "United States persons" then the judge must review the certification that the surveillance is necessary or essential, and the minimization procedures apply. These added safeguards, in my judgment, should prevent abuse.

Therefore, this amendment would provide that corporations or associations having a substantial number of members who are citizens or resident aliens cannot be excluded from "U.S. person" protection if they are alleged to be part F foreign powers, to be in the category of part F foreign power.

Now, that pretty well says it.

Senator CASE. Does that "more substantial" part have any meaning like more than half?

The CHAIRMAN. It could be less than half and more than a few.

Senator CASE. You mean like two is a group now?

The CHAIRMAN. Well, it would depend on the size of the group. If the group is four, then two would be substantial. If the group was 400, 2 wouldn't be substantial.

Senator CASE. If the group was three, one would be substantial.

The CHAIRMAN. That is probably accurate. What we are trying to do is if an incidental American is involved, we are not as concerned as if there are——

Senator CASE. If it is 1 against 99, that would be insubstantial?

The CHAIRMAN. That would be insubstantial.

Senator CASE. Insubstantial; OK.

The CHAIRMAN. Is there further discussion of five? Shall we skip on to six, or move on to six?

AMENDMENT No. 6

These two amendments make the seven judges members of a special court, as recommended by the Administrative Office of U.S. Courts, and provide fixed, staggered terms for the judges.

Amendment 6-a. Page 10, line 25, delete "each of whom" and substitute—"who shall constitute a special court, each member of which".

Amendment 6-b. Page 12, after line 8, add the following—"(d) Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, provided that the judges first designated under subsection (a) shall be designated for terms of from one to seven years so that one term expires each year, and that judges first designated under subsection (b) shall be designated for terms of three, five, and seven years."

These two amendments are relatively easy to deal with. They make the seven judges under this bill members of a special court and they provide fixed, staggered 7 year terms for the judges who are designated under the bill to issue orders and hear appeals.

Both amendments, let me say, are in line with recommendations by the chief counsel of the Administrative Office of the U.S. Courts in testimony last month before the House Intelligence Committee.

We were advised that the original structure flew in the face of all decorum as far as the way the Administrative Office of the U.S. Courts thought that the thing ought to be done, and I think this amendment conforms to what is procedurally accurate, and we don't harm our thrust.

Are there further discussions on six?

If not, we will turn to seven.

AMENDMENT NO. 7—CERTIFICATION REVIEW PROCEDURE

These two amendments clarify the judge's authority to review the certification that information sought from surveillance of a U.S. person is deemed to be foreign intelligence, and provide that he may seek additional information regarding the basis for such certification.

Amendment 7-a. Page 13, lines 23–24, delete and substitute—"(A) that the certifying official deems the information sought to be foreign intelligence information;"

Amendment 7-b. Page 17, line 6, add after "(E)"—"and any other information furnished under section 2524(c)."

Now, these two amendments clarify the judge's authority to review the certification that information sought from surveillance of a U.S. person is deemed to be foreign intelligence information, and provide that he may seek additional information regarding the basis for such certification.

This has been a cause celebre, really, from the beginning, to make certain that the certification process was real and had meaning. Under the bill, as reported by the Judiciary Committee, the certification procedure requires a high executive official to certify "that the information sought is foreign intelligence information." However, the original definition of "foreign intelligence information" stated that it was information deemed essential or necessary. Now, this would mean as a matter of pure logic that the only thing being certified was that the high official deemed the information to be essential or necessary. In cases of U.S. persons, and here again, we are talking about U.S. persons, the judge is required to review the certification to insure it is not "clearly erroneous." However, the way the bill has been worded, as a matter of pure logic, all the judge would review is whether an appropirate official deemed the information to be necessary or essential, and not whether that determination itself is clearly erroneous. The first part of this amendment makes clear the intent that the judge should do the latter.

It should go more than to make sure that the matter was deemed, which is relatively easy and simple to prove, but he should also go to the basic kinds of information that were sought.

The second part of the amendment follows up on a proposal made by our distinguished colleague from North Carolina, Senator Morgan, in the public hearings, where he asked the Attorney General to make sure the judge can get more information if he needs it to review the certification. It doesn't do much good to say that we are going to permit you to review the certification and then not give authority to get information necessary to make the reviewing.

Is there discussion on amendment 7?

[Pause.]

Senator CASE. Mr. Chairman, I think some little development of the report for this amendment's purpose would be desirable.

The CHAIRMAN. Well, if the Senator from New Jersey wants to propose that amendment, the chair and others, I am sure, will be prepared to give it full consideration.

Im sorry, the report? Fine.

I was thinking about 8 here.

AMENDMENT NO. 8—90-DAY EXECUTIVE REVIEW OF FOREIGN POWER SURVEILLANCE

This amendment requires 90-day review within the Executive branch for surveillances of so-called "official" foreign powers (parts A–C of the foreign power definition), which may last a year before renewal by the judge. This conforms with current administration procedures governing such surveillances. Without this amendment, the administration intends to review these surveillances only once a year.

Page 19, line 17, add after "less"—"provided that the Attorney General and the certifying official or officials shall review the certification at least every ninety days."

I have given that a lot of thought, and here again, it is a delicate balance to make sure that meaningful review occurs, that if we make this review occur at too frequent an interval, the tendency I think is going to be to make the review more superficial, so I am not going to initiate this. If someone else wants to they may. The fact of the matter is that the Executive branch now provides this 90-day review without legal requirement that they do so.

To be perfectly honest with you all, we have been advised that if we pass a law requiring a lesser review, they are going to make a lesser review. I am going to suggest that we require a review of this kind of particularly annually so we will not pursue the 90-day review with the understanding that elsewhere in the bill they are required to review and report to us every 6 months.

Senator CASE. We can say that, too, if you want, in the report.

The CHAIRMAN. The 6 months will be a matter of law. I mean, they have to review not only in-house, but they have to review in-house and then report to us every 6 months, and here again it is the balance of how much detail and how much of a review you are going to require to get the job done without requiring so much that it becomes a matter of rote not involving any thought process. That is what concerns me about the 90 days provision.

Now, I don't intend to say more. We may pursue this now or later, and if anybody wants to offer it, they may.

On amendment 9 we are talking about compliance with the minimization procedures.

AMENDMENT NO. 9—COMPLIANCE WITH MINIMIZATION PROCEDURES

These two amendments make clear the judge's authority to review compliance with the minimization procedures, and provide that information may only be used in accordance with such procedures.

Amendment 9-a. Page 20, line 2, add the following—"At the end of the period of time for which an electronic surveillance is approved by an order or an extension issued under this section, the judge may assess compliance with the minimization procedures required by this chapter."

Amendment 9-b. Page 21, line 22, add after (F)—"and in accordance with the minimization procedures required by this chapter."

The two parts of this amendment make clear the judge's authority to review compliance with the minimization procedures, and provide that information about U.S. persons may only be used in accordance with those procedures.

It just seems to me that we are talking about one of the most important aspects of this bill. You talk about how you collect, what you collect, and against whom do you collect, but the really critical question is what do you do with that information when you get it. So this is an important area.

As to the first part of this amendment, it has been suggested that the judge already has implicit authority to review compliance with all aspects of his order. However, it is useful in this case to spell out his authority explicitly so that the executive branch will have no doubt, and will not be able to question, that a judge may review the manner in which information about U.S. persons is being handled.

The second part clarifies another ambiguity. The section of the bill on "Use of Information" says, on page 21 at lines 17 to 22, that information concerning U.S. persons may be used and disclosed by Federal officials without the person's consent "only for purposes specified in section 2521(b)(8)(A) through (F)." That reference is to the "purposes" set forth in the definition of "minimization procedures." However, this is not the same thing as saying that the information must be used "in accordance with minimization procedures." I think this amendment tends to clarify that, and thus I recommend it to you.

The matter has been pretty well resolved with the exception that those who feel that the word "shall" instead of "may" should be used, as is contained in the amendment.

Is there further discussion?

We will move on to 10, the disapproved emergency surveillance.

AMENDMENT NO. 10—DISAPPROVED EMERGENCY SURVEILLANCE

This amendment further restricts the use of information about U.S. persons acquired from an emergency surveillance that a judge later disapproves.

Page 21, line 13, add after "thereof"—"; and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General where the information indicates a threat of death or serious bodily harm to any person."

This amendment, of course, amends the restriction on using information acquired from an emergency surveillance that a judge later disapproved, In other words, something happens quickly, you go out and act on the emergency provisions, and later on you find out that that action was wrong. As currently written on page 21, lines 4 through 13, the restriction says only that information acquired from such dis-

approved emergency surveillance may not be used in legal proceedings. It does not cover the use of information for other purposes.

What this amendment would do is to say OK, we recognize emergency situations. You make a good faith effort to do what is right. It conforms to the emergency provisions, but in the final analysis you find out that you acted wrongly under the emergency provisions; you should be unable to use this information in any way, not just say you can't use it in a court of law.

Is there further discussion there?

Let's move on to amendment 11.

AMENDMENT NO. 11—CLARIFICATION OF PRETRIAL NOTICE REQUIREMENT

This is a technical change to conform with the Judiciary Committee amendment, appearing on page 22, lines 15–16, which applies the pretrial requirement of notice to a court to state and local proceedings.

Page 22, line 12, add after "Government"—"of the United States, of a State, or a political subdivision thereof".

This is really a technical change to conform with the Judiciary Committee amendment that appears on page 22, lines 15 through 16. It applies the requirement of pretrial notice to a court of any anticipated use of the fruits of surveillance to State and local proceedings, which the Judiciary Committee chose to cover.

In other words, we are not just talking about Federal notice or Federal provisions or political subdivisions thereof. We are talking about State or political subdivisions.

Is there further discussion?

AMENDMENT NO. 12—USE OF UNINTENTIONALLY ACQUIRED PRIVATE DOMESTIC RADIO COMMUNICATIONS

This amendment is needed because part (C) of the electronic surveillance definition covers only the "intentional acquisition" of private domestic radio communications. Such communications may include telephone calls transmitted by radio-microwave. This amendment restricts the exploitation of such communications, if they are acquired "unintentionally."

Page 26, add after line 14—

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

Amendment 12, here we are talking about private domestic radio communications that are unintentionally acquired, and this amendment adds a new subsection (g) to the section on "Use of Information." It would be inserted on page 26, after line 14. The amendment is needed because part (C) of the definition of "electronic surveillance," beginning on page 7 at line 10, covers only the "intentional acquisition" of the contents of private domestic radio communications. Such communications may include telephone calls transmitted—well, could conceivably include communications such as the telephone calls that are transmitted by radiomicrowave, CB band transmissions, and the like.

Concern has been expressed by witnesses before the committee that this could be a major loophole in the bill. Unless the use of such "unintentionally acquired" phone calls is restricted, there would be a

potential abuse if the Executive branch adopted a vacuum cleaner approach for acquiring these kinds of domestic communications, without intentionally targeting any particular communication.

The amendment closes this possible loophole by restricting the use of any information acquired this way. If the Government unintentionally acquires through the use of any surveillance device the contents of a private domestic radio communication, where all the parties are located in the United States, these contents must be destroyed upon recognition. The only exception is with the Attorney General's approval where the contents indicate a threat of death or serious bodily harm to any person.

Is there further discussion on 12?

Let's turn to 13, then, if you please.

Senator CASE. Mr. Chairman, can I ask a very elementary question?

The CHAIRMAN. The question just asked was in that same category.

Senator CASE. Back on page 21 of our draft bill, at section 2526, the "Use of Information," this is just a matter, perhaps I don't get the significance of the language. It says under (a): "Information concerning U.S. persons acquired from an electronic surveillance conducted pursuant to this chapter may be used and disclosed by Federal officers and employees without the consent of the U.S. person only for purposes specified in" these subdivisions, and the amendment is proposed, of course for the minimization procedures, "or for the enforcement of the criminal law if its use outweighs the possible harm."

How can use outweigh? Maybe there is an explanation?

Mr. ELLIFF. This change was made at the request of the Justice Department in the original bill last year because they are concerned to indicate that within the Executive branch, there must be deliberation as to whether or not the possibility of disclosure of information in law enforcement proceedings, in legal proceedings, would pose a risk to the national security because of the sensitivity of the means by which that information was collected. It might, in other words, compromise a technique that is being used to collect that information. Therefore, this provision which is addressed not to the court, but rather to the executive officials who are implementing this bill, is one which requires a deliberative process.

Our report language and the Judiciary Committee report language previously says that the Attorney General should be involved in this deliberation at all times. However, he would not have the final say as to whether the use of the information outweighed its risks to national security. The final say would always be with the President, in weighing the law enforcement need over and against the risk of compromising a very valuable technique if we should use the information in court for law enforcement purposes.

That is my understanding of the intent of this provision.

Senator CASE. Well, I just wondered if we couldn't get a little better language, if the need for it, or its value, something of that kind, because if its use, its use can't outweigh, if you see what I mean.

Mr. ELLIFF. I will take that up with the Justice Department.

Senator CASE. If you would, I think that would make it a little more clear.

Mr. ELLIFF. I will take that up with the Justice Department.

Senator CASE. Mr. Chairman, I appreciate your permitting me to nitpick, but it does seem to me we ought to have it as secure as possible.

The CHAIRMAN. A good point.

AMENDMENT NO. 13—CONGRESSIONAL OVERSIGHT

This amendment insures that the Intelligence Committees are kept fully and currently informed. All but the first sentence parallels the similar provisions in the earlier bill reported in 1976.

Page 26, after line 24, add the following—

"§ 2528. *Congressional Oversight*

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

Back on 13, I am going to ask unanimous consent to change the wording, so that instead of "on a quarterly basis," I am going to suggest we put that on a semiannual basis.

Now, what we are talking about is the very critical, important oversight function, and we have two basic questions. One is how often should the oversight process take place? In other words, how big a burden are we placing on the Justice Department and the Attorney General. And two, how detailed must that report be, and as far as I am concerned, I am prepared to say do it semiannually, but do it fully. The Justice Department might not want the word "fully" in there, not because they are unprepared to give us information that we might ultimately feel that we need, but that they are concerned that on its face that might mean that every time they are to report, they, under the oversight provisions, they have to bring a truck up to the committee door; and I think we can in the report language point out that "fully" is designed to require that the Attorney General and the Justice Department give us all the information that is necessary to give us a complete picture, an accurate and honest picture of what is going on, and then "fully" comes in to give us the opportunity in the event we have questions, to be able to seek additional information and elaborate further on the information that is given to us by the Justice Department.

I think this oversight provision is critical, and for us to give the appearance to the public that we don't want to be fully briefed I think is conveying the wrong impression. I don't think it is good for us, and in the final analysis, I don't think it is good for the Attorney General, and I would hope that we could reconcile the differences there in the amendment where the committee agrees that it is not necessary every 90 days to have the people march up here and give us oversight, that they can do that twice a year, and in the process, we want to have the opportunity to get other information beyond what might be in the additional reporting.

I would hope that our staff could work with the Justice Department and find whatever language is necessary and put it in the report to accomplish in more succinct manner than I have just accomplished, describing what I would like to see be the thrust of this.

Senator CASE. I wonder, Mr. Chairman, whether the quarterly or semiannual or anything else specificity is the proper thing as opposed to "shall keep this committee currently informed."

The CHAIRMAN. We are talking about—I think we may be talking about different things.

Senator CASE. I am not sure that I am not.

The CHAIRMAN. Well, it is a reasonable question because the mission before us, we have so many irons in the fire here it is difficult for me to keep them all straightened out.

Here we are talking about the regimented kind of oversight that must take place under this electronic surveillance bill. Pursuant to this statute——

Senator CASE. Right.

The CHAIRMAN. It does not go to the responsibility that the Government has, various agencies have, to notify us instantly on the occurrence of certain other kinds of activities.

Senator CASE. Covert activities. I understand. But I just wonder whether—this would seem to relax with respect to surveillance, electronic surveillance, the other standards which applied to all major activities which might well include, it might very well involve or consist of electronic surveillance.

The CHAIRMAN. If the kind of activity involved here involve the kinds of sensitive things that could prove embarrassing and could get our country in trouble, they are required under Senate Resolution 400 to report it to us.

Senator CASE. I would be very happy to leave it quarterly in here if we could put in, you know, our intention not to negate——

The CHAIRMAN. Well, why don't we put that in there because we certainly don't want to negate those provisions, but if we have a full and complete overview every 6 months of what is actively going on, we could get a feel for what the problem is generally and whether the statute is being enforced, whether it goes too far, not far enough, but in addition to that, you have something that conforms to every dot and every title in this law, that is going to have the effect to blow the lid off of something particularly sensitive, we want to be advised of that.

And of course, as you know, both the Justice Department and the CIA and the other intelligence agencies have, I think have been very good to let us have this information.

Senator CASE. I am not criticizing our relationship with them currently at all.

The CHAIRMAN. And I think frankly, some of the rather spirited opposition to the way this provision is worded was not directed at their unwillingness to do it, because they are doing it now absent any requirement, but they hated to write that all down there and put themselves into a straightjacket, and I would hasten to say, I think most all this opposition has disappeared now. I think we are fairly close here to resolving this in a good manner.

HATHAWAY AMENDMENT RE CONGRESSIONAL OVERSIGHT

Section 2528. Congressional Oversight

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

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

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

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

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

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

Senator Hathaway's amendment on oversight, I think, is good to include here. This is another provision contained in that 1976 version of the bill. As you may recall, that provision requires that this committee report each year to the Senate concerning the implementation of the bill, including any necessary amendments, and it requires that any amendment proposed by the committee be considered promptly.

I guess that what it means is that we are going to require the various intelligence agencies to participate in the oversight process with us. We are going to require us to participate in the oversight process with the Senate. It is the same as last year.

I think that is a good amendment.

I hope that we will have further discussion of it.

AMENDMENT NO. 14—BELL SYSTEM LINE CHECKS

This amendment is proposed by the administration and restricts the practice of the Bell System to inform customers who request a line check whether or not there is a tap on their line.

Page 29, line 17, add after "2520."—"No communication common carrier or officer, employee, or agent thereof shall disclose the existence of any interception under this chapter or electronic surveillance, as defined in chapter 120, with respect to which the common carrier has been furnished either an order or certification under this subparagraph, except as may otherwise be lawfully ordered."

Fourteen deals with telephone line checks, and basically it is urged by the administration and would restrict the practice of the Bell System to inform customers who request a line check whether or not there is a tap on their line.

In essence, no communication common carrier or employee thereof shall disclose the existence of any wiretap under this bill if the common carrier has received a court order or emergency certification for the wiretap, unless otherwise lawfully ordered.

I think that is all right. We will go along with that. Is there any further discussion on that? If not, now, 15.

AMENDMENT NO. 15—TESTING AND DEFENSIVE "SWEEPS"

These two amendments ensure that testing and defensive "sweeps" must be conducted under procedures approved by the Attorney General and that defensive "sweeps," like testing, may not be targeted against a particular U.S. person without his consent.

Amendment 15–a. Page 30, line 8, add after "duty"—"under procedures approved by the Attorney General".

Amendment 15–b. Page 31, line 2, add after "provided"—"that no particular United States person shall be intentionally targeted for such purposes without his consent,".

This amendment discusses sweeping devices. This amends the provisions of the bill, appearing on pages 30 to 31, that excludes from the requirements of the bill any electronic surveillance for testing purposes or to conduct defensive sweeps to detect illegal surveillance devices.

The first part requires that such testing and defensive sweeps be conducted under procedures approved by the Attorney General. It is already administration policy under Executive Order 12036 on intelligence activities.

The second part of the amendment applies to defensive sweeps, the safeguard added by the Judiciary Committee to the testing provision. This safeguard provides that no particular U.S. person shall be intentionally targeted without his consent.

Again I think that is just sort of a housekeeping amendment, but it does deal with one very small possibility of abuse.

Is there discussion on that?

If not, we will go to amendment 16 about overseas surveillance exceptions.

AMENDMENT NO. 16—CLARIFICATION OF OVERSEAS SURVEILLANCE EXEMPTION

This amendment is proposed by the administration and ensures that the bill does not affect NSA's authority to acquire foreign intelligence from either international or foreign communications, except for the targeting of U.S. persons who are in the United States covered by this bill.

Page 31, line 13, add after "international"—"or foreign".

I have mixed feeling on this, but my feeling is that it is important for us to move forward on this bill and it does not deny us the opportunity to move forward in this area independently, an opportunity which I hope we will take advantage of.

I think this amendment helps give us the kind of support we need for a bill that is a pretty important piece of legislation.

This amends the provision of the bill there on page 31 at lines 9 through 14 that says that nothing contained in this bill or in the Communications Act of 1934 shall be deemed to affect the acquisition by the U.S. Government of foreign intelligence information from international communications by means other than "electronic surveillance" as defined in this bill.

The administration urges that this be clarified to include both international and foreign communications. This change makes no substantive difference in the bill, but it does reassure primarily the National Security Agency that its foreign activities are not restricted by this bill.

Is there further discussion? If not, 17, if anyone wants to take that up on their own, we will listen and consider it carefully. I frankly don't plan to offer it at this time, thinking that any foreign person who is an agent of a foreign power is significantly distinct from a citizen of this country that the constitutional prohibition from discrimination does not apply.

AMENDMENT NO. 17—CIVIL SUITS BY FOREIGN VISITORS

This amendment provides that the civil remedies of the bill are available to foreign visitors who are not officers or employees of a foreign power, as was the case under the earlier bill reported in 1976. As currently drafted, the bill denies civil remedies to certain foreign visitors who are agents of a foreign power.

Page 32, line 23, add after (A)—(i).

Shall we go back to 3 and 4, do we have time?

Senator CASE. Well, I'm sorry. I thought we were going to take these up again.

The CHAIRMAN. All right. Well, fine, why don't we leave it for the purposes of the public record for people who may be interested.

Senator CASE. And I would like to put in a comment that Mr. Levine makes at this point in the record. I hate to leave, but now I have stayed too long.

The CHAIRMAN. Well, I understand.

Senator CASE. I am terribly interested.

The CHAIRMAN. Well, if you have no objection, I will ask that the description of amendments 3 and 4, which are closely related, be made a matter of the record, and that the product there will be disseminated to anyone who is interested in looking at them.

Senator CASE. You are very kind and I appreciate it.

[The information referred to follows:]

AMENDMENT NO. 3—"FOREIGN INTELLIGENCE INFORMATION"

The definition of "foreign intelligence information" provides the standard for Executive branch certification that each surveillance is required. This amendment changes that definition so that it remains strict for information about "U.S. persons," but is lower for information about foreign powers and foreign persons. In the absence of this amendment, there is a danger that the protections for U.S. persons would be watered down in order to serve the purpose of justifying surveillance of foreign powers and foreign persons.

The amendment also drops the distinction between "necessary" and "essential" in the standard for information concerning U.S. persons. The differences between the two terms are only marginal, and using a single term has advantages of clarity and consistency.

Information concerning U.S. persons is "foreign intelligence information" if it is necessary to the national defense or security, to the successful conduct of foreign affairs, or to the ability to protect against grave hostile acts, sabotage, terrorism, or clandestine intelligence activities.

Information concerning foreign powers and foreign persons is "foreign intelligence information" if it relates to those interests.

Consideration was given to a standard of "important," rather than "relates to," for the more nebulous national defense, national security, and foreign affairs interests. We studied this matter very carefully, because we do not want to impose a standard that is so strict that Executive officials cannot honestly certify that entirely proper and appropriate activities are conducted to produce "foreign intelligence information," as defined here. For example, we realized that information is sometimes sought because it might become important if a crisis arises in the future. But there might be a doubt, or someone might raise a question, as to whether the information meets the "important" standard. Therefore, we concluded that the "relates to" standard is better where the information concerns foreign powers.

Significant safeguards still remain. First of all, the information must pertain to a "foreign power or foreign territory." It cannot simply be information about a foreign individual who is visiting the United States. Moreover, in the foreign affairs area, the information must relate to "the successful conduct of the foreign affairs of the United States." As for the term "national defense or the security of the Nation," the subject matter should clearly involve military concerns. Otherwise, the catch-all term "national security" could mean just about anything the Executive branch wanted it to mean.

With these safeguards in mind, then, the Committee can adopt a "relates to" standard without authorizing improper international conduct or improper treatment of foreign persons who come to the United States. The Committee's oversight authority is, of course, another very valuable check.

AMENDMENT NO. 4—DEFINITION OF "MINIMIZATION PROCEDURES"

The first part of this amendment is a minor technical style change. The second part replaces that part of the definition of "minimization procedures," on page 9 at lines 3–22, which was added by this Committee to the earlier version of the bill in 1976.

The minimization procedures are a vital part of the bill, because they regulate the acquisition, retention, and dissemination of information about U.S. persons who are not the authorized targets of surveillance. For example, an entirely innocent U.S. person might use a telephone that is tapped to target someone else. Or an American might talk on the phone to a foreign official who is under surveillance.

The procedures also protect Americans who are not parties to a conversation, or communication, but who are referred to in the communication.

The minimization procedures must be tight enough to prevent abuses, but not so complex as to be impossible to administer. We have found that the procedures developed in 1976 would, in some cases, be too complex to administer. This is the case with the procedures dealing with foreign-controlled entities, at lines 9–22. It may also be the case with the limits on how information is retained.

Therefore, the amendment concentrates on the main problem—the dissemination of information—where abuses are most likely to occur. It also focuses on those types of information which are the hardest to pin down concretely—that is, information which relates solely to the national defense or security and the conduct of foreign affairs.

The amendment requires procedures which are reasonably designed to insure that such information is not disseminated in a manner which identifies a U.S. person, without that person's consent, unless the person's identity is necessary to understand or assess the importance of information with respect to a foreign power or foreign territory.

The phrase "with respect to a foreign power or foreign territory" comes from the definition of "foreign intelligence information." The words "necessary to understand" mean that the U.S. person's identity is needed to make the information intelligible. If the information can be understood without identifying the U.S. person, it should be disseminated that way. However, sometimes it might be impossible or difficult to make sense out of the information without the U.S. persons' identity. For example, to take an obvious case, if the message says a foreign government official is arriving in this country at a particular time and place, it would be necessary to identify the airline he is arriving on. The airline company falls in the definition of "U.S. person," because it is a U.S. corporation substantially made up of U.S. citizens.

This example also shows why it is not appropriate to adopt the same standard as the "foreign intelligence information" definition, because it would be hard to establish that this information is "necessary to the national defense or the security of the Nation" or "necessary to the successful conduct of the foreign affairs of the United States." Instead, it is useful information that would be entirely proper to disseminate.

On the other hand, if the information concerns a phone conversation between a U.S. Senator and an Ambassador, the information could always (or perhaps I should say almost always) be understood by deleting the Senator's identity.

The other standard for dissemination is that the U.S. person's identity must be necessary to "assess the importance" of information with respect to a foreign power. By "importance," we mean important in terms of the interests set out in the definition of "foreign intelligence information." For example, if a foreign coun-

try is negotiating with an American business firm to purchase nuclear materials, it might be important to the national defense or security (in a military sense), or to the successful conduct of the Government's non-proliferation policy, to know the identity of the business firm involved. That might be the only way the State Department could determine whether a deal is likely to be made. On the other hand, the information may turn out not to be important. The question under the bill is whether the identity of a U.S. business firm or businessman is needed to assess that importance.

Of course, none of these are hard-and-fast lines. What the bill requires is careful deliberation by responsible officials in the Executive branch. The court is also there to monitor compliance with the minimization procedures, in order to deter abuses. There are going to have to be judgment calls, and that is why the bill says the procedures must be "reasonably designed" to limit dissemination under these standards.

CASE AMENDMENT—"UNITED STATES PERSON" DEFINITION

This amends the definition of "United States person," which now includes corporations or associations having a substantial number of members who are U.S. citizens or permanent resident aliens, unless such corporation or association is a "foreign power."

There is a problem with this exception, because it means that groups substantially composed of U.S. citizens or resident aliens do not have the same protections as U.S. persons, if they are alleged to be covertly directed and controlled by a foreign government under part (F) of the "foreign power" definition.

Part (F) of the "foreign power" definition includes any "entity" that is directed and controlled by a foreign power, even if the entity is substantially composed of citizens. There is concern that this might be used as a way to by-pass the criminal standard for surveillance of individual Americans, by tapping instead the group they belong to.

However, if such entities substantially composed of Americans are "United States persons," then the judge must review the certification that the surveillance is necessary or essential, and the minimization procedures apply. These added safeguards should prevent abuse.

Therefore, this amendment provides that corporations or associations having a substantial number of members who are citizens or resident aliens cannot be excluded from "U.S. person" protections if they are alleged to be part (F) foreign powers.

The CHAIRMAN. Well, find a day that we can all be here next week, and resolve this, and I will ask the staff to find out when that day is and to advise me how much additional time we are going to need, because we are talking about not only considering it but getting the report prepared. And I know you fellows are working 48 hours a day and you have had enough of it this week.

All right.

Mr. Levine, do you have anything to add to our deliberations as a surrogate for our colleague from New Jersey? Will you do that for the record?

Mr. LEVINE. So long as the record shows that the Senator from New Jersey does have an amendment, in addition to the amendments that were passed out.

The CHAIRMAN. I am aware of the Senator's amendment, and will consider it carefully.

All right, let me again say to all who are here, first to our staff who has labored diligently, I think has done a yeoman job of resolving as nearly as we can what appeared some time ago to be irreconcilable difference, how much the chairman of the committee is in your debt, and also to those private and Executive branch citizens that are here, we are in your debt for the efforts you made, not only to inform us of what the facts and problems really are, but the tolerance which

I hope will continue in sufficient quantity that we can get this bill through, because it is important. We all know that. And without the help of the many of you who do not wear an official hat as far as this committee is concerned, we couldn't be close to where we are right now, which is very close to getting this bill moved out, and I suggest or predict that it will pass. Thank you.

[Whereupon, at 12:33 p.m., the committee recessed, subject to the call of the Chair.]

MONDAY, FEBRUARY 27, 1978

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, D.C.

The committee met, pursuant to notice, at 10:25 a.m., in room 318, Russell Senate Office Building, Senator Birch Bayh (chairman of the committee) presiding.

Present: Senators Bayh (presiding), Huddleston, Morgan, Inouye, Goldwater, Case, Garn, Pearson, Chafee, and Lugar.

Also present: William G. Miller, staff director; Earl Eisenhower, minority counsel; Audrey Hatry, clerk of the committee.

The CHAIRMAN. Gentlemen, while we are waiting for a quorum to come—we have had nine. One of our brethren went to Foreign Relations, and he is on his way back here—we might take just a minute or two just to discuss a procedural question.

Would there be objection, once we get a quorum to accept a motion and vote on a motion that would report out the bill, as amended, pending the opportunity to poll the committee members on each amendment that was considered?

Senator GOLDWATER. I don't see anything wrong with that, Mr. Chairman, because I don't think there is a person here that doesn't have at least three other committees we could be at. That procedure is not unusual. This is not a measure that we are unacquainted with. So I would move that we proceed on that basis.

The CHAIRMAN. Well, I will hold the vote on that motion in abeyance until one more live body walks into the room.

Senator GOLDWATER. Senator Pearson was here.

The CHAIRMAN. He is on his way back here. He was here and had to go to Foreign Relations.

Senator GARN. Maybe you had better just say one more body rather than a live body awaiting a quorum.

The CHAIRMAN. Jake, if you see any other kind of body walk in the door, let me know.

We have about 15 amendments before us this morning that I might put into the record, some background of this bill without bothering the committee on it because you all claim to be aware of it, and we have lived through it together.

We went over all but two of these amendments last Friday. The remaining two are amendments 3 and 4. No. 3 is a revised definition of "foreign intelligence information." No. 4 is the amendment to the definition of minimization procedures. On this issue, Senator Case has an alternative amendment, and the administration has asked us to consider a change in the version of amendment No. 4 that we have before us. It would be a relatively minor change. As far as I know, it is

acceptable, at least part of it is acceptable, but to put it all on top of the table, that would be a little different from what we have had before us over the weekend.

All of the other amendments, including No. 3, have been accepted by the administration, and inasmuch as at least I am one of the prime movers of those amendments, have been accepted by some of us on this committee.

In some cases they were proposed by the administration. In all other cases they have been drafted in close consultation with the administration, the individual agencies and the private groups who are concerned about the bill.

As I said the other day, it would be wrong to suggest that just because there has been a signing off, an agreement, that all the parties to the agreement are completely happy. They are not. I think we have melded together an understanding that in this area it is very difficult to accomplish the goal of national security and the goal of individual protection without a great deal of tolerance and understanding, and I will say to the private groups and to the agencies, the public individuals, representatives of our Government as well as those that are concerned that our Government do the right thing, looking at it from outside, that there has been a great deal of cooperation, and I want to thank again all those involved.

Now, if there is no objection—well, how does the committee care to proceed? Do you want to go down these one at a time again, repeat the ones we went over the other day, or go to 3 and 4, the ones that we didn't go over the other day?

What is the committee's pleasure?

Senator GARN. Might I just suggest that we start with No. 1 with a brief explanation, particularly those that we already went over, and have a vote on them, and the ones that we did not discuss obviously will take a little longer.

The CHAIRMAN. All right.

That is not an unusual request. It is a mark of good sense from our colleague from Utah.

Why don't we turn to amendment 1. We have here an explanation that has been prepared that goes just a little bit more in detail that I worked on over the weekend, and perhaps instead of just reading the small definition and trying to expand on it, it might save time to just go into the bit more precise and detailed explanation.

If you look to amendment 1 there, as we see—now, this is the definition of "agent of a foreign power" on page 3 at lines 6–19 of the bill, if you want to look at this bill. This part of the definition applies only to persons who are not U.S. persons, that is, not citizens or permanent resident aliens.

Obviously there are two separate paragraphs. Paragraph (i) deals with officers or employees of a foreign power. As reported by the Judiciary Committee, this paragraph reads "is an officer or employee of a foreign power." The problem with this wording is that it includes anyone who is employed by his government in his home country, and visits the United States in a purely private capacity. For example, a French bus driver technically is employed by his country, but he visits this country as a tourist, as a citizen, certainly he should not be in-

cluded in the province of our intelligence gathering mechanism. That is not the kind of person we intend to cover.

So the amendment substitutes the words "acts in the United States as an officer or employee of a foreign power." This excludes the tourist who just happens to fall into the definition of the previous wording.

Now, paragraph (ii) is the standard for surveillance of foreign visitors who are not acting as officers or employees of a foreign power in this country.

I see a quorum, and my special thanks to the Senator from Kansas for making two efforts to be with us this morning, and I regret the inconvenience this has caused him.

Senator PEARSON. Thank you, Mr. Chairman.

Go right ahead.

The CHAIRMAN. Jim, we had the motion made by our distinguished friend from Arizona that the committee be permitted to consider these amendments one at a time and to vote on them, and then have the committee polled and the product of that then be reported out to the Senate.

Is there objection to that procedure?

The Chair sees none. We will note that the quorum is present and unanimously supported that vote.

Senator GARN. We appreciate these lame ducks coming around to help us out.

Senator PEARSON. Lame turkey.

The CHAIRMAN. Unless there are objections, the Chair will interpret the Senator from Arizona's motion as a move to report the bill as amended.

Senator GOLDWATER. That's right.

Senator HUDDLESTON. Second.

The CHAIRMAN. All in favor say aye.

[A chorus of ayes.]

The CHAIRMAN. Opposed, no.

[No response.]

The CHAIRMAN. Thank you, gentlemen.

Now, in the second paragraph, this is the standard for surveillance of foreign visitors who are not acting as officers or employees of a foreign power in this country. Under S. 3197, the earlier version of the bill which the committee reported last year, such foreign visitors were covered under the same standard that applies to U.S. persons. However, S. 1566, as proposed by the administration and reported by the Judiciary Committee, sets a lower standard for all foreign visitors to the United States. In my judgment, this lower standard is broader than necessary to deal with the FBI's very legitimate foreign counterintelligence requirements. Therefore we have worked with the FBI and the Justice Department to develop a new standard that is tailored directly to the FBI's requirements.

First of all, the person must be acting for or on behalf of a foreign power which engages in clandestine intelligence activities contrary to the interests of the United States. Persons acting for such foreign powers are covered in two situations.

They are covered when the circumstances of their presence in the United States indicates that they may engage in such activities, that

is harmful clandestine intelligence activities in the United States. For example, the FBI may know from past experience that a particular foreign power uses a certain class of visitors to this country for carrying out secret intelligence assignments. If a visitor falls in this class, it is not necessary to show that he actually has an intelligence assignment.

As good an example as I have found is that our Russian friends seem to like to use middle-aged Russians who come to this country as students but whose background shows that they have a high degree of training in certain technical skills. Now, that category that classification in the past, has had a very high degree of people who we are able to prove fit into this definition and thus that class would be permitted under this particular language, where the circumstances are suspect.

Visitors acting for such powers are also covered when they knowingly aid or abet any person in the conduct of harmful clandestine intelligence activities, or when they conspire with any person knowing that such person is engaged in such activities.

That aid and abet standard is always a difficult one, but here you have to do more than aid and abet, you have to know that the person you are aiding and abetting is engaged in such activities.

Now, that is perhaps a longer definition than we need, or description than we need of amendment 1.

Is there further discussion on that, please, gentlemen?

Senator GARN. I just make a comment, Mr. Chairman, that initially under the first standard, I thought that was too restrictive and would allow the Soviets to specifically use tourists and so on, in fact, would drive them to use them, but I think (ii) clarifies it and I am willing to accept the amendment.

The CHAIRMAN. I know you looked at that very carefully, and I appreciate your support.

Senator CHAFEE. May I ask a question, Mr. Chairman?

When you have got that language in there, that he engages in clandestine intelligence activities contrary to the interests of the United States, now suppose somebody is trying to get blueprints of a naval ship of ours. It seems to me that is clandestine intelligence activities, but do you then have to go on and show that it is necessary to the interests of the United States? It seems to me the very definition of clandestine intelligence activities is contrary to the interests of the United States.

Do you have to go prove that it in some manner is contrary to our interests?

The CHAIRMAN. Yes. The touchy problem right there is the lobbying question, of certain kinds of legitimate lobbying activity should not be included.

Senator GARN. May I clarify this, Mr. Chairman?

I think the thing you have to look at here, the first part of this, it is the country, not the individual we are talking about, acts for or on behalf of a foreign power which engages in clandestine intelligence activities contrary to the interests of the United States. The Soviet Union does that. That is a known fact. So that is establishing that the country does this, not the individual.

Then the individual, you go to the second part of it, indicates such person may engage in such activities in the United States and knowingly aids or abets, and so we are talking about—we discussed this

Friday, two different things. That is the country, and that is already established. There are lists that——

Senator CHAFEE. How about France? How about somebody from France that we catch engaging in—well, from France. Is that a country which engages in clandestine intelligence activities contrary to our interests?

Senator GARN. I don't know whether they are on the list or not. There is a list of countries that do this. Whether they are on the list, I don't know.

The CHAIRMAN. It would be a factual situation there. Unfortunately it is not an unusual activity, I suppose, for our friends or for us to be involved in certain kinds of activity in friendly nations that fall into this category, but it would have to be the kind of activity described here, which it seems to me pretty well restricts it the way in which we want to restrict it. You have to be acting for or on behalf of the intelligence service, and the interest has to be contrary to the interests of the United States.

Senator CHAFEE. Well, I thought all of that modified "foreign power" rather than the individual or his actions.

The CHAIRMAN. If you go down further and indicate that such person may engage in such activities in the United States, we talk about both the kind of activity and the damage.

Senator CHAFEE. I see. OK.

Senator GARN. What you are really saying is that just because somebody works for a foreign government and the government fits that "contrary to interests," you can't bug them unless they—unless it is indicated that they are participating.

Senator HUDDLESTON. You are going to have to have a little knowledge about the person and why he is here.

The CHAIRMAN. Well, you see, I think it is important for us to understand that you can always get at these people, foreign visitors, under the same standard that you can apply electronic surveillance to American persons. In this particular instance we are lowering the standard a little bit, which makes it possible for us to deal with certain kinds of people.

In other words, the circumstances are such that you have a higher degree of probability that they are participating in this kind of activity than would normally be the case. John, if I read into your concern that this would make it—this is not sufficiently strong or is worded in a way which would make it difficult to get to people who are really damaging, this would be a lower standard.

Senator CHAFEE. My concern is that we are making it awfully tough to get after someone from a foreign—I regret raising this at this time because I know you gentlemen spent a lot of time, and I haven't, on this, so I am not going to raise any other question if I can help it because you gentlemen put a lot more time into this than I did.

Senator HUDDLESTON. One thing, John, it seems to me it lowers the threshold considerably. For instance, if we know the Soviet Union is engaged in espionage against our technical collection in this country and all of a sudden they send a man over here who is an expert in that particular field, that almost is an indication that he is here for the purpose of furthering that collection. Any person whose presence here

indicates that he might be here to help ongoing or what we know a country is doing in this thing.

Senator CHAFEE. OK. I am satisfied, Mr. Chairman.

The CHAIRMAN. You see, we had two. If you had a person who we know is an officer or an employee of a foreign power, in other words, we know we are talking about an intelligence agent, then you have no question, so that part that you were worried about is where you do not know. This is a person who is not an official, maybe someone that comes over with a foreign delegation, or the student example where we have a pretty good idea to believe that in that class of people, more often than not you are going to have a very high degree of agents. But this is a lower standard than that directed at U.S. persons, to make it easier to reach this kind of person than if it was a U.S. person.

I tell you, if you think it is confusing, you have a lot of company. At least one other member of this committee shares that.

Senator GARN. Well, I think the main point here, though, is it may not be as loose as some people want, but it does reduce the standard for a foreign visitor from that of an American citizen.

The CHAIRMAN. That's right, that's right. This is a lower standard than applied to other people, not a higher standard. It is a lower standard.

Are there further comments?

Senator GARN. I move approval of amendment No. 1.

Senator GOLDWATER. Second.

The CHAIRMAN. Are there objections to the motion to report amendment No. 1?

The Chair hears none.

We will go to amendment No. 2.

This amends the second part of the definition of "agent of a foreign power" from page 3 at line 20 to page 4 at line 23. This part of the definition applies to any person including a U.S. person. The main purpose of this amendment is to establish a criminal standard for surveillance of U.S. persons.

This in my judgment is the one amendment that was the most difficult to work out, yet the most important from the standpoint of how you balance protecting civil liberties on one hand, versus making it possible for intelligence forces to function on the other.

Let me just go through a brief description of what we are talking about here in each paragraph.

Paragraph (i) deals basically with spying. It covers any person who 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. This is a significant improvement over the previous noncriminal standard of the bill reported out by the Judiciary Committee.

Paragraph (ii) deals with a more nebulous area, "any other clandestine intelligence activities." This is basically covert political action by a foreign intelligence service. The term is so vague, however, that it could border on political activities protected by the first amendment. Therefore, the standard is stricter than for spying in two respects. First, the person must act pursuant to the direction of an intelligence service or network of a foreign power. Second, the activities must involve or be about to involve a Federal crime. These added safeguards

are needed to protect persons who are primarily exercising their first amendment rights.

We have that—I might point out that Senator Biden's amendment which has been added to this protects a U.S. person or persons who are merely exercising their first amendment rights by providing that no U.S. person may be considered an agent of a foreign power solely on the basis of activities protected by the first amendment. In other words, anyone who is involved in some of the concerns involving certain national groups in this country and how that impact is on foreign power when they talk to us from out home and urge us to get involved or write us letters, that would be automatically excluded from this definition.

Senator HUDDLESTON. That absolves us, Members of the Senate, who are constantly being accused of being agents of foreign powers when we take certain positions on certain legislation.

The CHAIRMAN. Or people back home who urge us to take those positions. I mean, if you are not careful, you could get people that are really exercising first amendment rights enmeshed in this net, and we don't want that.

The third paragraph deals with sabotage or terrorism, and frankly, this turned out to be the hardest to draft, not because anybody wants to be easy on sabotage or terrorism, but getting the information available in a timely fashion so that in addition to arresting someone after the fact, you have a reasonable opportunity to prevent the act from happening makes it more difficult to deal with.

As proposed by the administration and reported by the Judiciary Committee, the standard is "knowingly engages in activities that involve or will involve sabotage or terrorism for or on behalf of a foreign power." The problem with this standard is that the words "will involve" require a high degree of certainty that terrorism will take place, especially when compared with the "may involve" standard for spying. Therefore, we have tried to draft a standard that is more realistic. The language of the proposed amendment reads, "knowingly engages in sabotage or terrorism, or activities which are or may be in preparation thereof, for or on behalf of a foreign power."

The term "preparation" does not require evidence of preparation for a specific terrorist act, because the definition of terrorism, as you recall, speaks of violent acts and means a range of acts, not just one specific act, a pattern. So you don't have to nail it down to one particular incidence of violence or sabotage or terrorism.

Preparation normally means preparation for a specific kind, which therefore caused a problem because it could be too strict under certain circumstances. In this bill, however, the term "preparation" would not have its normal meaning because of the special definition in the bill as far as terrorism is concerned. It could reasonably be interpreted to cover, for example, providing the means for the commission of acts of terrorism rather than one particular bombing or the act itself.

Paragraph (iv) includes the aiding or abetting and conspiracy standard of the bill, as reported by the Judiciary Committee, by making clear that the person must knowingly aid or abet any person in the conduct of the activities described, not merely aiding and abetting, but knowing really the consequences of that aiding and abetting.

Now, gentlemen, that perhaps is a longer explanation than is needed, but let me tell you, it just skims the surface of the effort that has gone into that particular amendment.

Senator GARN. Mr. Chairman, as you well know from over 2 years of working on this bill, I have been opposed to a criminal standard because it simply, in my opinion, restricted the intelligence-gathering agencies from doing what I felt was a legitimate job of foreign intelligence.

However, despite that objection, I will be able to, I should put in the word "reluctantly," support (i) on the basis that one word is put in and that is "may involve" a violation. If we did not have the word "may," I will be very frank about it, I would do everything I could to delete this section and this amendment, but I can reluctantly support it with the word "may" there.

On (iii), I don't object to the word "preparation" if we do adequately describe what you have just done in the report language.

The CHAIRMAN. We must do that.

Senator GARN. So we do not leave a lot to interpret what the word "preparation" means, and have the judges overly restrict that word.

So with that word "preparation" in proper report language, I can also support (iii).

The CHAIRMAN. Well, Senator Garn has been closely involved as the ranking member on the Right of Americans Subcommittee for a long period of time. As he pointed out—and I appreciate his concern and I appreciate his willingness to be a part of this process to meld together those who had differing ideas, "may" I think is an important part of that process, plus I will ask staff in structuring this language, if there is no objection, to make certain that Senator Garn is consulted with the report language that we arrive at. It has got to tie in the definition of terrorism there.

Is there objection to reporting amendment 2?

[No response.]

The CHAIRMAN. The Chair hears none.

Amendment 3, this goes to the definition of "foreign intelligence information." It provides the standard for executive branch certification that each surveillance required. This amendment changes that definition so that it remains strict for information about U.S. persons, but is lower for information about foreign powers and foreign persons. In the absence of this amendment, there is a danger that the protections for U.S. persons would be watered down in order to serve the purpose of justifying surveillance of foreign powers and foreign persons.

Now, just quickly, we know that our Constitution requires that foreign persons be accorded the same kind of protections as individual Americans unless the circumstances are sufficiently critical or distinct that a reasonable distinction could be made, and it seems to me that in this area where we are talking about foreign intelligence and the protection of the country, that we will not have a constitutional question, but I think out of fairness the committee needs to know that this is a question that we have considered.

The amendment also drops the distinction between "necessary" and "essential" in the standard for information concerning U.S. persons. Frankly, the differences between the two terms are marginal, perhaps

negligible, and using a single term has advantages of clarity and consistency.

If you read that original bill, some was necessary, some was essential, back and forth. What we have done is we have just put in, necessary to the national defense or security or the successful conduct of foreign affairs, or the ability to protect against grave hostile acts, sabotage, terrorism, or clandestine intelligence activities, so it reads in a uniform manner. You needed to go back and forth from one section to the other to try to figure out what was necessary and what was essential, so we are just going to use "necessary" through there.

Information concerning foreign powers and foreign persons is foreign intelligence information if it relates to those interests. Now, we did make that distinction, relates to foreign powers and foreign persons.

Consideration was given to a standard of "important" rather than "relates to," for the more nebulous national defense, national security, and foreign affairs interests. We studied this matter very carefully because we do not want to impose a standard that is so strict that executive officials cannot honestly certify that entirely proper and appropriate activities are conducted to produce "foreign intelligence information" as defined here. For example, we realized that information is sometimes sought because it might become important if a crisis arises in the future. But there might be a doubt, or someone might raise a question, as to whether the information meets the important standard now, as of this moment, when you have to make the test. Therefore we concluded that "relates to," the "relates to" standard is better where the information concerns foreign powers.

Significant safeguards still remain, let me hasten to say. First of all, the information must pertain to a "foreign power of foreign territory." It cannot simply be information about a foreign individual who is visiting the United States. Moreover, in the foreign affairs area, the information must relate to the successful conduct of the foreign affairs of the United States. As for the term "national defense or the security of the Nation," the subject matter must clearly involve military concerns. Otherwise, the catchall term "national security" could mean just about anything the executive branch wanted it to mean.

With these safeguards in mind, then, the committee can adopt a "relates to" standard without authorizing improper international conduct or improper treatment of foreign persons who come to the United States. The committee's oversight authority is, of course, another very valuable check in this regard.

Senator GARN. Mr. Chairman, I would just comment briefly here that this is another amendment that I have had trouble with because of the definition concerning "foreign" people. The original intent of this entire legislation was primarily to protect American citizens, and I felt the original draft carried those protections too far to foreign nationals and people that could be involved in espionage.

So again, on the basis of setting a lower standard for foreigners than for our own citizens, I can support this amendment.

The CHAIRMAN. Thank you.

Are there objections to reporting amendment No. 3?

[No response.]

The CHAIRMAN. Amendment 4 is a rather—it is not that long an amendment but it has significant consequences, and we thus perhaps

ought to take 3 or 4 minutes to explain it because in my judgment it is crtical. The first part is a minor technical change. The second part replaces that part of the definition of "minimization procedures," on page 9 at lines 3 to 22, which was added by this committee to the earlier version of this bill in 1976.

So let's just look at it. First of all minimization procedures are a vital part of the bill because they regulate the acquisition, retention, and most importantly, the dissemination of information about U.S. persons who are not the authorized targets of surveillance. We are talking about Americans who are inadvertently swept up into the intelligence gathering process.

The procedures also protect Americans who are not parties to a conversation or communication but who are referred to in the communication, which is an even one step further inadvertent sweeping into the intelligence collection system.

The minimization procedures must be tight enough to prevent abuses, but not so complex as to be impossible to administer. We have found that the procedures developed in 1976 would, very frankly, in some cases, be too complex to administer. This is the case where the procedures dealing with foreign-controlled entities, at lines 9 through 22. It may also be the case with the limits on how information is retained.

Therefore, the amendment concentrates on the main problem, the dissemination of information, where abuses are most likely to occur. It is not just how you get it or what is there, but the person is hurt when that information is disseminated. It also focuses on those types of information which are the hardest to pin down concretely; that is, information which relates solely to the national defense or security and the conduct of foreign affairs.

The amendment requires procedures which are reasonably designed to insure that such information is not disseminated in a manner that identifies a U.S. person without that person's consent, unless the person's identity is necessary to understand or assess the importance of the information.

The phrase "with respect to a foreign power or foreign territory" comes from the definition of "foreign intelligence information." The words "necessary to understand," of course, means that the U.S. person's identity is needed to make the information intelligible. If the information can be understood without identifying a U.S. person, it should be disseminated that way. However, sometimes it might be impossible or difficult to make sense out of the information without the U.S. person's identity. For example, to take an obvious case, if the message says a foreign government official is arriving in this country at a particular time and place, it would be necessary to identify the airline he is arriving on.

The airline, in many instances, under the definitions in this bill, would be a U.S. person. This example also shows why it is not appropriate to adopt the same standard as the "foreign intelligence information" definition, because it would be hard to establish that this information is "necessary to the national defense or the security of the Nation" or "necessary to the successful conduct of the foreign affairs of the United States." Instead, it is useful information that would be entirely proper to disseminate.

Other standard for dissemination is that the U.S. person's identity must be necessary to assess the importance of information with respect to a foreign power. By "importance" we mean important in terms of the interests set out in the definition of "foreign intelligence information." For example, if a foreign country is negotiating with an American business firm to purchase nuclear materials, it might be important to the national defense or security, in a military sense, or to the successful conduct of the government's nonproliferation policy, to know the identity of the business firm involved. That might be the only way the State Department could determine whether a deal is likely to be made or not. On the other hand, after the investigation is consummated, the information may turn out not to have been important after all. The question under the bill is whether the identity of a U.S. business firm or businessman is needed to assess that importance.

Of course, none of these are hard and fast lines. What the bill requires is careful deliberation by responsible officials in the Executive branch. The court is also there to monitor compliance with the minimization procedures, in order to deter abuses. There are going to have to be judgment calls, and that is why the bill says the procedures must be reasonably designed to limit dissemination under these standards.

Now, I would like to ask consent that in addition to the——

[Pause.]

The CHAIRMAN. I have been advised over the weekend—this is a constant process of trying to keep everybody happy, or at least keep everybody in business, I suppose I should say—that the administration feels that it would significantly lower their procedural problems as to the dissemination or lack of authority to disseminate if we could also include at the end of the amendment with respect to foreign power or foreign territory the following, "such information is otherwise publicly available."

"Or", "Or such information is otherwise publicly available," and then, although they would like to have the following, "or such person is incumbent of any office of the executive branch of the U.S. Government having significant responsibility for the conduct of the U.S. defense or foreign policy," I am about of the opinion that that could better be handled in the report language in a way that would deal with the particular problem that concerns the administration.

In other words, we would say that if the information is otherwise publicly available, we would not prohibit its dissemination.

Is there further discussion about amendment 4 and what we are trying to do there?

[No response.]

The CHAIRMAN. I there any objection to adding to that amendment the clause about publicly available information?

[No response.]

The CHAIRMAN. Is there objection to accepting amendment 4?

[No response.]

The CHAIRMAN. The Chair hears no objection.

I think the record should show that Senator Case would object there. That is in the packet of information that you have been given. He had an amendment which he discussed the other day, so the committee is privy to his reasoning.

94-628 O - 76 - 15

Amendment 5. This amendment provides that a group substantially composed of U.S. citizens or resident aliens shall have the same protection as U.S. persons, even if they are alleged to be covertly directed and controlled by a foreign government under part (F) of the "foreign power" definition.

Here again what we are trying to do is to see that wherever you have a group or an organization in this country that has significant numbers of American citizens within it, that the standard be that of U.S. persons so that you provide the kind of protections that we want to afford U.S. persons.

Senator HUDDLESTON. Have you pinned down "substantially" yet?

The CHAIRMAN. The best we can do is nebulous, as the Senator from Kentucky knows, but the Justice Department is willing to report language that says more than a few and less than a majority.

Yes, Senator Chafee?

Senator CHAFEE. No, no.

The CHAIRMAN. Is there objection to amendment No. 5?

[No response.]

The CHAIRMAN. Gentlemen, I have to say, we all know we are dealing with business that is not an exact science. You get tired of hearing me say this is not a 2 plus 2 equals 4 business. If it were, we wouldn't have these problems. I appreciate your tolerance in helping provide the fractions.

Amendment No. 6 amends to make the seven judges designated, to issue orders under the bill, members of a special court and provide fixed, staggered 7-year terms for the judges designated under the bill to issue orders and to hear appeals.

Both amendments, frankly, are in line with and really are the result of concerns expressed by the Chief Counsel of the Administrative Office of the U.S. Court in testimony expressed to the House Intelligence Committee last month, and also in personal discussions with our committee. This seems to be the form in which judicial matters should be structured.

Is there objection to amendment 6?

[No response.]

The CHAIRMAN. The Chair hears none.

Amendment No. 7 goes to the certification review procedures. Perhaps I should give you the background a bit more in detail than that short summary because this is an important matter. These two amendments clarify the judge's authority to review the certification that information sought from surveillance of a U.S. person is deemed to be foreign intelligence information and provide that he may seek additional information regarding the basis for certification.

Under the bill as reported by the Judiciary Committee, the certification procedure requires a high executive official to certify, and I quote, "that the information sought is foreign intelligence information." However, the original definition of "foreign intelligence information" stated that it was information "deemed" essential or necessary. This would mean, as a matter of pure logic, that the only thing being certified was that the high official deemed the information to be essential or necessary. In cases of U.S. persons, the judge is required to review the certification to insure that it is not "clearly erroneous."

However, the way the bill has been worded, as a matter of pure logic, all the judge would review is whether an appropriate official deemed the information to be necessary or essential, and not whether that determination itself is clearly erroneous. The first part of this amendment makes clear the intent that the judge should do the latter and review the determination made by the official, not just that the "deemed" be reviewed.

The second part of this amendment follows up on a proposal made by Senator Morgan in the public hearings where he asked the Attorney General to make sure the judge can get more information if he needs it to review the certification.

In other words, what we want to be reviewable here is the thought processes and the conclusions that were reached, and if the judge is not satisfied, to be able to ask the executive official for more information to substantiate that executive determination.

Is there further discussion?

Senator LUGAR. Mr. Chairman, just as a question in review, there are only seven judges who will be involved in this procedure, if I read this correctly, and three of these, then, form this board of review if there is a question raised about the decision of one of the seven.

The CHAIRMAN. That is accurate.

Senator CHAFEE. Well, the three don't come from the seven, do they?

The CHAIRMAN. There are actually 10 altogether. The seven——

Senator LUGAR. The three are outside.

The CHAIRMAN. Is there further discussion?

[No response.]

The CHAIRMAN. Is there objection?

Senator CHAFEE. Can you go to whomever you choose?

Is there a rotating——

The CHAIRMAN. Well, the court is given the authority to establish that procedure. I think we ought to have some language in the report discussing or dealing, if we want, with the rotation procedure, if this does not present us with an administrative problem.

That has been in the Judiciary Committee report. I think it should be in ours.

Senator CHAFEE. What? That they rotate?

The CHAIRMAN. That they give serious consideration to the rotating procedure. I don't know what kind of an administrative problem it creates, John. If it doesn't, I think that is what it should be, so that you cannot have the judge shopping temptation.

Senator CHAFEE. This, of course, is in addition to their regular duties, isn't it, the district court judges.

The CHAIRMAN. That is accurate.

Senator LUGAR. Mr. Chairman, is the procedure, just once again, in the rudimentary sense, that the Attorney General initiates these requests so that the physical locations of the judges is not an important factor here. Presumably the Attorney General will be here in Washington and so will the seven judges or one of the seven that is to be approached as well as the three outside of these who would review a denial, and the idea is they would all be rather close at hand as opposed to somebody in the field in San Francisco requesting surveillance permission.

The CHAIRMAN. Well, at the time the request has been made, certainly the Justice Department anticipates that that judge in question will be here. I think it is fair to say that this is not going to confine the choice of judges to people in the District of Columbia, but during the process they will certainly be here.

Senator LUGAR. But physically it is reasonable to suspect that if there is a geographical distribution in the selection, that if the judge that is sitting, let's say, in Idaho normally, he would fly to Washington, D.C., and hear the appeal by the Attorney General physically here in this city.

The CHAIRMAN. Yes; or it could be—well, that is why we want to leave this procedural mechanism up to the court. I think they suggested they would like to have that opportunity. They might parcel it out so that certain judges had a 1-month stint, so they would come and hear all requests during the month, or 2 months or whatever it might be, so that it wouldn't be a shuttle.

Senator LUGAR. So that time would not be a factor in case of emergency. In other words, I am just raising a hypothetical situation that some cases might be more urgent than others, and if you have a rotation that you have to take Idaho, Iowa, Arizona, and so forth, and the judges that are coming in, this may create a procedural difficulty for an emergency, a terrorism type situation, for instance, as opposed to——

The CHAIRMAN. Well, the way this is anticipated in the conversations we had is that there would be someone in the box at all times. It might be someone from Idaho who is sitting during that period, assigned to him, but that you wouldn't have to go shopping all over the country in an emergency situation, which I think you are absolutely right.

Senator LUGAR. Well, maybe the report can reflect this, that the committee contemplates that there is someone literally on call, physically present so the time is not a factor, that the Attorney General can within minutes approach the judge to get a decision.

The CHAIRMAN. I think that is important, and John, why don't you, after you prepared that, review it with Senator Lugar to make certain that he is confident. It's a good point.

Amendment 9, the two parts of this amendment dealing with minimization procedure, compliance. They make clear the judge's authority to review compliance with the minimization procedures and provide that information about U.S. persons may only be used in accordance with such procedures.

In the first part, it has been suggested that the judge already has implicit authority to review compliance with all aspects of this order. However, it is useful in this case to spell out his authority explicitly so that the Executive branch will have no doubt, and will not be able to question that a judge may review the manner in which information about U.S. persons is being handled.

The second part clarifies another ambiguity. The section of the bill on use of information says on page 21 at lines 17 through 22 that information concerning U.S. persons may be used and disclosed by Federal officials without the person's consent "only for purposes specified in section 2521(b)(8) (A) through (F)." That reference is to the purposes set forth in the definition of minimization procedures. How-

ever, this is not the same thing as saying that the information must be used in accordance with the minimization procedures. This amendment makes sure that we are talking about the same thing, here again giving the judge unquestioned authority to review to see that the minimization procedures are operating as we intended.

Is there objection to amendment 9?

The Chair hears none.

Was there objection to amendment 7? I didn't hear that.

Amendment 10? I think perhaps the best way to deal with amendment No. 10 is just to read the amendment. This amendment further restricts the use of information about U.S. persons acquired from an emergency surveillance that a judge later disapproves, the kind of situation that Senator Lugar pointed out, and it reads "and no information concerning any United States person acquired from such surveillance shall subsequently be used." In other words, if you have an emergency situation where you act in good faith but on reflection and study it turns out not to have been the proper action, then the information acquired will not be used.

Well, yes; there is one exception and that is where the approval of the Attorney General is necessary and where the information indicates a threat of death or serious bodily harm to any person, where it is necessary to warn the person involved.

Is there further discussion?

[No response.]

The CHAIRMAN. Are there objections?

[No response.]

The CHAIRMAN. The Chair hears none.

Amendment 11, this is a technical change to conform with the Judiciary Committee amendments appearing on page 22, at lines 15-16. It applies to requirement of pretrial notice to a court of any anticipated use of the fruits of surveillance to State and local proceedings, which the Judiciary Committee chose to cover.

Further discussion on 11?

[No response.]

The CHAIRMAN. Objections to 11?

[No response.]

The CHAIRMAN. The Chair hears none.

Twelve, which is the use of unintentionally acquired private domestic radio communications, adds a new subsection (g) to the section on the use of information, and it would be inserted there in the draft on page 26, after line 14. The amendment is needed because part (c) of the definition of electronic surveillance beginning on page 7 at line 10 covers only the intentional acquisition of the contents of private radio communications. Such communications may include telephone calls transmitted by radio-microwave, and we wanted to make sure that this is not a major loophole, so this amendment would cover unintentionally acquired phone calls.

Senator GOLDWATER. Let me ask a question about that. It is almost impossible that it could happen, but let's say a person interested in communications, be he a licensed operator or just a shortwave listener, should tune in on a station which—it would have to be operating unknowingly—were transmitting in the clear and uncoded way and he heard material that he felt would be of value to our Government.

Would that be unintentional, and would the person involved—this has probably never happened, but occasionally I talk to Russians in code who are not supposed to talk to United States citizens, code or otherwise, and such a situation could possibly arise, and I am just wondering if the operator reported this information to any intelligence agency would the person involved be involved under this amendment?

The CHAIRMAN. Well, first of all, to apply this amendment, the parties involved would all have to be in the United States. Second—staff, correct me if I am wrong—but this does not deal with the kind of unintentional information which is learned by a private person. We are talking about governmental types of procedure.

Senator GOLDWATER. I just wanted to get that clear because it has never happened in my life of communicating, but it could.

The CHAIRMAN. Well, we have been told by the Executive branch, and I think it is accurate, and by the agencies involved that this kind of—to use one of my favorite terms, vacuum cleaner approaches of gathering intelligence is not used here at our people, but this is in the event that sometime that might change.

Senator GOLDWATER. I just wanted to protect my brothers.

The CHAIRMAN. OK.

Further discussion on 12?

[No response.]

The CHAIRMAN. Objection?

[No response.]

The CHAIRMAN. The Chair hears none.

Now amendment 13 deals with Congressional oversight. Very quickly, it does three things. First, it requires the Attorney General to fully inform the Intelligence Committee of the House and Senate concerning all electronic surveillance under this chapter. He must do so on a semiannual basis. Second, the amendment adopts language similar to that contained in the earlier version of the bill reported by this amendment in 1976. It makes clear that nothing in the bill shall be deemed to limit the authority and responsibility of those committees to obtain such additional information as they may need to carry out their respective functions.

Third, Senator Hathaway has suggested, and it is appropriate to include here, in my judgment, another provision contained in the 1976 version. That provision requires this committee to report each year to the Senate concerning the implementation of the bill, including any necessary amendments which are required as a result of experience. It requires that any amendments proposed by the committee be considered promptly.

There are a couple of points here. First of all, the original requirement was a 90-day reporting, and the administration was concerned about what "fully" means. We sort of had a little tradeoff here in which we used "fully" but went to semiannual reporting to the Congress, and then gave us the authority to look beyond this report and to seek additional information if it was necessary to clarify what we had been given.

Is there further discussion?

Senator LUGAR. Mr. Chairman, in the semiannual reporting, is it understood that among appropriate questions to the Attorney General would be how many surveillance activities occurred?

The CHAIRMAN. Yes; that is accurate.

Senator LUGAR. For example, to get some idea of the frequency as well as whether the procedures worked out. It seems to me the quantity of the activity would be important.

The CHAIRMAN. Yes. That is why we were rather insistent on "fully." We just don't want a great volume of information that has no meaning to it. We want to really have an ability to provide intelligent intelligence oversight.

And I should say on behalf of the administration, the people down at Justice who were concerned about this is that this, their concern was more a technical concern. It in no way evidenced an unwillingness on their part to really provide this information, but I think they would have been more comfortable to do it on a voluntary basis rather than have it written in.

I think we have resolved this to everybody's satisfaction.

Senator CHAFEE. Mr. Chairman, when you say "shall fully inform," not when you say, when the bill says, the amendment says, would you envision that they would come and report on the specifics of the taps that they are on, for example, we are tapping here, there, everywhere?

The CHAIRMAN. I think that first of all we would require, I think the committee has established this procedure and I would suggest strongly we follow it, that whatever information was given to us was not identified in such a way that it would disclose the person involved or the place involved, but that certainly we should have enough information so we would know the circumstances, so we would know just exactly what kind of invasion this is and exactly what kind of information we are seeking.

We could go into further detail if it seemed to be necessary to explain what was happening, but I think for our own protection we don't want to know this information unless it is absolutely necessary for fear it might jeopardize someone.

Senator CHAFEE. And would you envision the Attorney General personally coming before the committee and giving this report twice a year?

The CHAIRMAN. Well, either the Attorney General or his designee who is given this responsibility under this bill. It would be the Deputy, as I understand it.

Senator CHAFEE. Probably rather than a written report.

The CHAIRMAN. Yes. In the past the Attorney General has made the original report and then our staff has gone to the Justice Department to review. They have cooperated very, very satisfactorily with us, and I think it is important to understand that we have had a lot of voluntary cooperation from the Justice Department and the other agencies where they have given us information without it being mandated. We haven't had to cudgel them. But this is again, we are putting a law down there, let's look into the future, and I think these safeguards are necessary.

Further discussion on 13?

[No response.]

The CHAIRMAN. Any objection?

[No response.]

The CHAIRMAN. The Chair hears none.

Amendment 14, really it is urged by the administration and would restrict the practice of the Bell System to inform customers who re-

quest a line check whether or not there is a tap on their line. No communication common carrier or employees thereof shall, under this amendment, disclose the existence of any wiretap under this bill, if the common carrier has received a court order or emergency certification for the wiretap, unless otherwise lawfully ordered.

Senator GOLDWATER. This wouldn't restrict a citizen who suspects that his wire is tapped from asking the Bell Co. or any other company to surveil to determine?

The CHAIRMAN. No; it would not prohibit him from requesting it, but if this was a lawfully ordered warranted tap, he cannot be informed of it, even if they found it.

Senator GOLDWATER. Well, let's say he suspects it is tapped. The telephone company could say yes or no if it didn't involve an ordered tap.

The CHAIRMAN. That is correct.

I think staff points out the response would be there is no unauthorized tap on your line or there is an unauthorized tap on your line. There——

Senator CHAFEE. There is no unauthorized taps. There is just authorized taps.

The CHAIRMAN. That is basically what has been happening, and this is what this amendment would continue to do. I mean, if you have got some mafioso here and he wants his wire swept and he goes to the telephone company, I question whether we want them to say yes, you have a tap on your line. We have got a court order here. If the standards of this bill are sufficient to protect individuals who shouldn't be tapped, if someone falls into the suspect category and we conclude in this bill that they should be tapped, then it seems to me to be rather inconsistent to say that they ought to have advance warning of it, or should have warning of it if indeed they take the initiative on their own.

Senator GOLDWATER. I agree with that perfectly. It is just the fellow that wants to listen in.

The CHAIRMAN. Yes; but this would not deal with the fellow who was unauthorized. That would be alerted to that.

Senator LUGAR. Mr. Chairman, just in review, are there other laws that provide for tapping of telephones? In other words, when the customer calls in to Bell, is this the only case in which the Attorney General might have called for a line to be tapped, or does the FBI have some authority under some other legislation?

The CHAIRMAN. Title III of the omnibus crime bill of 1968 gives that warrant procedure which is avilable now. In this area there is no warrant procedure available.

Senator LUGAR. What is the procedure in that law when it comes to this amendment? Is it consistent?

The CHAIRMAN. This would cover both laws.

Senator LUGAR. Both.

The CHAIRMAN. Are there any further questions?

[No response.]

The CHAIRMAN. Is there objection?

[No response.]

The CHAIRMAN. The Chair hears none. We are coming along here, fellows.

Fifteen, this amends the provision of the bill appearing on page 30–31 that excludes from the requirements of the bill any electronic

surveillance for testing purposes or to conduct defensive sweeps to detect illegal surveillance devices. The first part requires that such testing and defensive sweeps be conducted under procedures approved by the Attorney General. This is already administration policy under executive order.

The second part of the amendment applies to defensive sweeps with a safeguard added by the Judiciary Committee to the testing provision. The safeguard provides that no particular U.S. person shall be intentionally targeted without his consent. In other words, the sweep mechanism as a defensive safeguard should not be permitted as an offensive tool.

Further discussion?

[No response.]

The CHAIRMAN. Objection?

[No response.]

The CHAIRMAN. The Chair hears none.

Amendment 16 goes to the clarification of overseas surveillance exemption, and I think that the description there in the information before us is appropriate. This amendment is proposed by the administration and insures that the bill does not affect NSA's authority to acquire foreign intelligence from either international or foreign communications, except for the targeting of U.S. persons who are in the United States covered by this bill.

Is there further discussion?

[No response.]

The CHAIRMAN. Is there objection?

[No response.]

The CHAIRMAN. The Chair hears none.

The bill will subsequently be reported pursuant to the motion of the distinguished Senator from Arizona, and my gratitude to all of you and to the staff that has worked awfully hard, and to those of you present who have had to bite the bullet on this one, you have been very helpful to us.

Thank you all.

Senator GOLDWATER. Mr. Chairman, I would like to have Senator Pearson to be recorded as aye.

The CHAIRMAN. Fine.

We will ask, if there is no objection, I think your motion at the beginning said or included the opportunity for other members to be polled.

Senator GOLDWATER. That's right.

The CHAIRMAN. We will ask the staff to do that.

[Whereupon, at 11:34 a.m., the committee recessed subject to the call of the Chair.]

APPENDIX A

LETTER FROM ATTORNEY GENERAL GRIFFIN B. BELL TO SENATOR MORGAN

SEPTEMBER 21, 1977.

HON. ROBERT MORGAN,
U.S. Senate,
Washington, D.C.

DEAR SENATOR MORGAN: During my testimony concerning S. 1566, you asked if the Department of Justice could provide you with a statement outlining the basis for the Department's conclusion that the President may approve warrantless electronic surveillance in the United States under certain circumstances.

In every case in which the issue has been directy raised, the decision has been that the President may lawfully approve warrantless electronic surveillances of foreign powers and their agents. *See United States* v. *Buck*, 548 F. 2d 871 (9th Cir. 1977); *United States* v. *Butenko*, 494 F. 2d 593 (3d Cir. 1974) (en banc); *United States* v. *Brown*, 484 F. 2d 418 (5th Cir. 1973); *United States* v. *Clay*, 430 F. 2d 165 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971); *United States* v. *Enten*, 388 F. Supp. 97 (D.D.C. 1971), *aff'd in part and vacated in part sub nom., United States* v. *Lemonakis*, 485 F. 2d 941 (D.C. Cir. 1973); *United States* v. *Hoffman*, 334 F. Supp. 504 (D.D.C. 1971). In *Buck*, the most recent case, the Ninth Circuit referred to such warrantless surveillances as a "recognized exception to the general warrant requirement." The Supreme Court has not addressed the question, but has taken pains to make clear that its decisions requiring warrants in other circumstances do not apply to surveillances involving foreign powers or their agents. *See Katz* v. *United States*, 389 U.S. 347, 358 n. 23 (1967); *United States* v. *United States District Court*, 407 U.S. 297, 308, 322 & n. 20 (1972).

In *Butenko*, the opinion which undertook the most substantial analysis of the issues involved, the Third Circuit initially determined that the President had as incident to his Article II powers the power to gather foreign intelligence information. 494 F. 2d at 601, 603. The court then determined that this power could be exercised only in accordance with the Fourth Amendment, 494 F. 2d at 603. The court recognized that the Fourth Amendment bars only unreasonable searches but acknowledged that a prior warrant is the normal test of whether a search is reasonable. Referring to other exceptions to the warrant requirement, however, the court weighed the costs of requiring a warrant against its benefits and determined that because of the need for secrecy and speed in foreign intelligence surveillances and the opportunity for occasional post-surveillance review, a warrant was not required. 494 F. 2d at 605. The court made clear that this exception only applies where the primary purpose of a surveillance is to gather foreign intelligence. 494 F. 2d at 606.

The holding of the District of Columbia Circuit in *Zweibon* v. *Mitchell*, 516 F. 2d 594 (1975) (en banc), is not inconsistent with *Brown* and *Butenko*. In *Zweibon* the court held that a prior judicial warrant was required for electronic surveillance of persons who were neither agents of nor collaborators with a foreign power. While in dictum a plurality of the court suggested that a warrant should be required even where the subject of the surveillance was an agent of a foreign power, the court made clear that its actual decision was not so broad.

In light of this case law and in the absence of statute, the Department of Justice has consistently maintained that reasonable surveillances conducted against foreign powers and their agents, personally authorized by the Attorney General pursuant to an express Presidential delegation of power, are lawful absent a warrant.

Yours sincerely.

GRIFFIN B. BELL.
Attorney General.

APPENDIX B

Office of the Attorney General
Washington, D. C. 20530

February 28, 1978

Honorable Birch Bayh
Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Enclosed is a copy of guidelines which I have approved regulating the dissemination of information obtained by the FBI through the use of extraordinary techniques.

Sincerely,

Griffin B. Bell
Attorney General

DISSEMINATION OF INFORMATION OBTAINED BY EXTRAORDINARY TECHNIQUES

The FBI is authorized by part IX B of the Foreign Intelligence Collection and Foreign Counterintelligence Investigation Guidelines to disseminate information obtained in the course of such investigations. This addendum to the Guidelines adds additional restrictions on the dissemination of information acquired by the use of extraordinary techniques. It supersedes paragraphs IX B 2.a. and b., and 4.a. and b. with respect to all information acquired by extraordinary techniques after its effective date.

The following restrictions are designed to prevent unnecessary dissemination of information acquired by extraordinary techniques particularly where the information identifies or permits identification of United States persons.[1] Certain specific needs to receive information from the FBI are identified in these guidelines. The FBI should ascertain other needs of agencies receiving foreign intelligence or counterintelligence information on a regular basis and should disseminate only that information which appears relevant to the official responsibilities of the agency receiving it. Receiving agencies should be instructed that no dissemination is to be made outside that agency without the consent of the FBI.

Where dissemination requires approval of the Director of the FBI or his designee, approval may be given only by supervisory officers at FBI Headquarters, designated in writing by the Director.

These guidelines do not restrict dissemination of information by the FBI, including identifying information, when necessary to the conduct of investigations within its jurisdiction.

These guidelines apply to all information acquired by extraordinary techniques under the foreign intelligence collection and foreign counterintelligence investigation guidelines after the effective date of this addendum.

I. Dissemination of Information for Foreign Intelligence Purposes

Information disseminated to other federal agencies for foreign intelligence purposes, which was gathered at FBI initiative, shall not identify or permit identification of United States persons, except by general characterization, unless the identification is essential to understand the information or to assess its importance.

Information gathered at the request of another agency may be disseminated to that agency in a form which identifies or permits identification if that agency requests such identification in writing, setting forth the basis for such request.

Any request by a receiving or initiating agency for identifying information shall be referred to the Director or his designee for a determination whether the identfication is essential to understand the information or assess its importance.

---

[1] As used herein, "United States person" means an individual who is a citizen of the United States or an alien admitted for permanent residence.

II. Dissemination of Counterintelligence Information

Information disseminated to other federal agencies in the intelligence community which have a direct counterintelligence interest in the information [2] may identify or permit identification of United States persons. Where the information is of interest to, but does not relate to the direct responsibilities of the receiving agency, United States persons may not be identified.

Any subsequent request by the receiving agency for identification of United States persons, generally characterized in the initial dissemination, shall be referred to the Director of the FBI or his designee for a determination whether the identification is relevant to a direct counterintelligence interest of the receiving agency.

III. Dissemination of Information Concerning Sources or Contacts

On specific request by name from other agencies in the intelligence community, the FBI may disseminate information concerning the suitability or credibility of sources or contacts of the requesting agency or persons who the requesting agency reasonably believes are potential sources of contacts.

IV. Dissemination of Information Relating to Criminal Activity

The dissemination of information relating to criminal activity which is acquired by extraordinary techniques during counterintelligence investigations or the collection of foreign intelligence information is subject to the following conditions:

A. Information pertaining to criminal activity may be disseminated to Federal, State or local agencies having investigative jurisdiction thereof or having responsibility to provide protection against such activity, with the concurrence of the Department of Justice, taking into account the following factors:

(1) the seriousness of the crime,

(2) the risk of compromising the source of the investigation, and

(3) whether the information is necessary to successful prevention, detection or prosecution.

B. Information pertaining to passport or visa fraud or attempted fraud may be disseminated to the Department of State.

C. Information disseminated under this provision may identify United States persons involved in the criminal conduct or those who are victims or potential victims of such conduct.

D. Any dissemination of information under this provision shall include a notice to the recipient that the information being furnished should not be used in connection with a prosecution or other judicial proceeding without the express written approval of the Department of Justice, after consultation with the FBI.

---

[2] There are three principal entities in the United States Government engaging in foreign counterintelligence activities: FBI, CIA and organizations within the Department of Defense designated by the Secretary of Defense. Since the National Security Council is responsible for the development and formulation of national intelligence activities pursuant to Executive Order, it is also a recipient for purposes of these guidelines. Likewise, the Department of State may be a recipient of information relating to international terrorism in carrying out its foreign affairs responsibilities.

V. Dissemination of Information Concerning Trustworthiness of Federal Employers and Persons Granted Access to Sensitive Information or Facilities

Information which raises a question about the trustworthiness of—
(1) a current federal employee,
(2) a former employee of an agency in the intelligence community,
(3) a person holding a security clearance or having access to sensitive information or facilities, or
(4) a person who held a security clearance for or was otherwise granted access to information classified as "Secret" or a higher classification,

may be disseminated to the Government employer or former employer, the agency which granted the clearance or access, or another federal agency having responsibility to investigate the trustworthiness of the individual. Dissemination of such information must be approved by FBI Headquarters. The information disseminated may identify the individual.

Information which raises a question about the trustworthiness of individuals who are applicants or prospective Government employees should not be disseminated until the FBI has verified the employer's official interest in the individual concerned.

VI. Dissemination to Congressional Committees

Information relating to foreign intelligence, foreign counterintelligence, or criminal conduct may be disseminated upon request to congressional committees having jurisdiction over such matters to the extent authorized by the Attorney General. If the information was collected at the request of, or in collaboration with another agency, that agency shall be consulted prior to the dissemination.

The information disseminated shall not identify or permit identification of United States persons, except by general characterization, unless the identification is essential to understand the information or assess its importance.

Any subsequent request by the receiving committee for identification of United States persons, generally characterized in the initial dissemination, shall be referred to the Attorney General or his designee for a determination whether the identification is essential to understand the information or assess its importance.

VII. Dissemination to Foreign Governments

A. Foreign intelligence

Dissemination of foreign intelligence information to foreign governments is not within the responsibility of the FBI. Any requests by another federal agency to the FBI for authority to disseminate foreign intelligence information obtained from the FBI which identifies or permits identification of United States persons shall be referred to the Attorney General or his designee for a determination whether the dissemination is in the interest of the security or foreign policy of the United States. Where there may be significant implications for U.S. foreign relations involved in the dissemination, the Department of State shall be consulted prior to approval of the dissemination.

B. Counterintelligence information

Counterintelligence information may be disseminated to a foreign intelligence or security agency when such dissemination is approved by FBI Headquarters as being in the interest of the security or foreign policy of the United States. Where there may be significant implications for U.S. foreign relations involved in the dissemination, the Department of State shall be consulted prior to dissemination. Any dissemination of such information to a foreign agency is subject to the following conditions:

1. When a request is initiated by a foreign agency for information on a named United States person, the FBI may disseminate information concerning that individual, and other United States persons whose identity is essential to understand or assess the importance of the information disseminated, only when such dissemination is in the interest of the security or foreign policy of the United States.

2. Information disseminated to a foreign agency at FBI initiative shall not identify United States persons, except by general characterization, unless there is information of direct interest to the receiving agency indicating that such persons is or may be engaged in clandestine intelligence activities pursuant to the direction of a foreign power.

3. Any subsequent request by the foreign agency receiving the information for identification of United States persons, generally characterized in the initial dissemination, shall be referred to the Attorney General or his designee for a determination whether identification is of direct interest to the foreign agency and dissemination is in the interest of the security or foreign policy of the United States.

C. Criminal information

Information relating to criminal activity may be disseminated to foreign law enforcement or security agencies having jurisdiction of the offense, subject to the following conditions:

1. Where there may be significant implications for U.S. foreign relations involved in the dissemination, the Department of State shall be consulted prior to dissemination.

2. Information pertaining to criminal activity may be disseminated to the appropriate agency of a foreign government, with the concurrence of the Attorney General or his designee, taking into account the following factors:

(a) obligations imposed on the United States by treaties or other international agreements,

(b) the seriousness of the offense,

(c) the risk of compromising the source of the investigation,

(d) whether dissemination of such information is in the interests of the United States.

3. Information disseminated under this part may identify United States persons involved in the criminal conduct or those who are victims or potential victims of such conduct.

4. Any such dissemination of information shall include a notice to the recipient that the information being furnished should not be disclosed publicly or disclosed to another government without the express written approval of the Department of Justice, after consultation with the FBI.

VIII. Protection of Life, Property, and Sensitive Information

The FBI may disseminate to another Federal agency information relating to activity directed at its personnel, premises or property when the activity may involve injury to persons, substantial damage to premises, property or material, or the loss or compromise of national security or important foreign policy information. The dissemination of such information may identify United States persons when necessary to protect against such activity.

The FBI may disseminate to a Federal, state or local agency information relating to activity directed at an international organization when the activity may result in injury to persons the receiving agency has an obligation to protect. The dissemination of such information may identify United States persons when necessary to protect against such activity.

Nothing in these provisions limits the authority of the FBI to inform individuals whose safety or property is directly threatened by planned violence or conduct dangerous to human life, so that they may take appropriate protective safeguards. In so informing such individuals, no identification of United States persons shall be provided unless identification appears necessary to insure safety.

IX. Dissemination Under Exceptional Circumstances

Where there are exceptional circumstances which indicate that dissemination of information acquired by extraordinary techniques not otherwise provided for is necessary, the FBI may disseminate the information with the prior approval of the Attorney General, made or confirmed in writing.

94-628 O - 18 - 16

APPENDIX C

Reprinted by permission of Charles G. La Bella, Associate Editor, Fordham University

NOTE

FOREIGN SECURITY SURVEILLANCE—BALANCING EXECUTIVE POWER AND THE FOURTH AMENDMENT

INTRODUCTION

Under the present state of the law, the President, based upon his own unilateral determination, may intercept any and all communications of persons he feels pose a threat to the national security. Despite recent attempts to provide effective, reasonable guidelines for requiring judicial authorization prior to intercepting such communications, no legislation has ensued.[1] The perennial stumbling block has been the difficulty encountered in striking a balance between the necessary and legitimate governmental use of electronic surveillance in protecting the national security and insuring the protection of personal liberties.[2] On March 29, 1976 the Senate Judiciary Committee began the fourth set of hearings on warrantless electronic surveillance in as many years.[3] The highlight of these hearings, the Foreign Intelligence Surveillance Act of 1976[4] (Foreign Intelligence Act) is the most recent, unsuccessful effort at striking a fair and just balance between these two competing interests.

The fourth amendment guarantees an individual the right to be free from unreasonable governmental searches and seizures.[5] The Supreme Court, in interpreting what has been termed an indispensible freedom,[6] " 'has em-

1. S. Rep. No. 1035, 94th Cong., 2d Sess. 9 n.2 (1976) [hereinafter cited as Senate Report], citing S. 743, National Security Surveillance Act of 1975, 94th Cong., 1st Sess. (1975); S. 1888, Bill of Rights Procedures Act of 1975, 94th Cong., 1st Sess. (1975); S. 2820, Surveillance Practices and Procedures Act of 1973, 93d Cong., 1st Sess. (1973); S. 4062, Freedom from Surveillance Act of 1974, 93d Cong., 2d Sess. (1974).

2. Senate Report, supra note 1, at 9, 11.

3. Id. at 9 n.3, citing Hearings on S. 743, S. 1888, S. 3197 Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary, 94th Cong., 2d Sess. (1976). [hereinafter cited as Senate Hearings]; Subcomm. on Surveillance of the Senate Comm. on Foreign Relations and the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary, Warrantless Wiretapping and Electronic Surveillance, 94th Cong., 1st Sess. (1975); Joint Hearings Before the Subcomm. on Administrative Practice and Procedure and the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary, Warrantless Wiretapping and Electronic Surveillance, 93d Cong., 2d Sess. (1974); Hearings Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary, Warrantless Wiretapping, 92d Cong., 2d Sess. (1972).

4. S. 3197, 94th Cong., 2d Sess. (1976) [hereinafter cited as the Foreign Intelligence Act].

5. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, 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." U.S. Const. amend. IV.

6. Almeida-Sanchez v. United States, 413 U.S. 266, 274 (1973), quoting Brinegar v. United States, 338 U.S. 160, 180 (1949) (Jackson, J., dissenting). Upon his return from the Nuremberg trials, Mr. Justice Jackson, greatly affected by the arbitrary governmental acts of the Nazi regime performed at the expense of personal liberties, wrote that "[t]hese [fourth amendment rights], I

phasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes[6] and that searches conducted outside of the judicial process . . . are *per se* unreasonable . . . ."[7] Review by an impartial judicial officer prior to a search or seizure has been the "time tested" method of effectuating fourth amendment protections,[8] and is subject only to a few carefully delineated exceptions.[9] Traditionally, however, the mandate of judicial process has been limited to those searches or seizures accompanied by an actual physical trespass, the absence of which precluded further fourth amendment inquiry.[10] It was not until 1967 that the Supreme Court, in *Katz v. United States*,[11] held that the spirit and protection of the fourth amendment cannot be limited by the presence or absence of physical trespass.[12] In removing this limitation the Court held that the electronic interception of private communications[13] constituted a search and seizure under the fourth amendment and

---

protest, are not mere second-class rights but belong in the catalog of indispensible freedoms. Among deprivations of rights, none is so effective in cowing a population, crushing the spirit of the individual and putting terror in every heart. Uncontrolled search and seizure is one of the first and most effective weapons in the arsenal of every arbitrary government." Id.

7. Katz v. United States, 389 U.S. 347, 357 (1967) (citation omitted), quoting United States v. Jeffers, 342 U.S. 48, 51 (1951).

8. United States v. United States Dist. Court, 407 U.S. 297, 318 (1972). "The Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised. This judicial role accords with our basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government." Id. at 317 (footnote omitted). See, e.g., Coolidge v. New Hampshire, 403 U.S. 443, 449 (1971); Katz v. United States, 389 U.S. 347, 356-57 (1967); Wong Sun v. United States, 371 U.S. 471, 481-82 (1963); Johnson v. United States, 333 U.S. 10, 13-14 (1948).

9. Almeida-Sanchez v. United States, 413 U.S. 266, 280-82 (1973) (Powell, J., concurring); United States v. United States Dist. Court, 407 U.S. 297, 318 (1972); Chimel v. California, 395 U.S. 752, 762-63 (1969); Terry v. Ohio, 392 U.S. 1, 20 (1968); Katz v. United States, 389 U.S. 347, 357 (1967); Jones v. United States, 357 U.S. 493, 499 (1958). It appears to be quite clear that the ultimate standard set forth in the fourth amendment is one of reasonableness. Cady v. Dombrowski, 413 U.S. 433, 439 (1973). Reasonableness turns only in part upon the warrant requirement. However, those instances which have been exempted from the warrant requirement have been based on exigent or other circumstances where delay would frustrate legitimate police activity. United States v. United States Dist. Court, 407 U.S. 297, 318 (1972) ("in general, [these exceptions] serve the legitimate needs of law enforcement officers to protect their own well-being and preserve evidence from destruction"); Jones v. United States, 357 U.S. 493, 499 (1958). Thus we are left with the conclusion that whenever practicable the test of reasonableness will require a judicial warrant prior to a search or seizure.

10. Katz v. United States, 389 U.S. 347, 352 (1967); Goldman v. United States, 316 U.S. 129, 134-36 (1942); Olmstead v. United States, 277 U.S. 438, 457, 464, 466 (1928).

11. 389 U.S. 347 (1967).

12. Id. at 352-53.

13. The term electronic interception or surveillance includes the interception of communications by means of "bugging" and "wiretapping." Bugging is a technique by which oral communications, not transmitted by wire, are intercepted. Wiretapping is a technique by which any communication (not necessarily oral) transmitted by wire may be intercepted. Both techniques are

was thus subject to its mandate of judicial process.[14] However, the Court has never held the warrant provision applicable to the President's use of electronic surveillance when employed for the purpose of gathering foreign intelligence information to protect the national security.[15] On the other hand, the Court has never specifically carved out an exception from the warrant provision for these national security surveillances.[16] In essence there is a gap in the

included in the term electronic surveillance as used within this Note unless a distinction is otherwise indicated.

14. 389 U.S. at 353. Prior to its decision in Katz, the Court had held that absent an actual physical trespass the use of electronic surveillance did not constitute a search or seizure for purposes of the fourth amendment. Olmstead v. United States, 277 U.S. 438 (1928). A bugging device must be implanted upon either the sender or receiver of the oral communication, thus requiring a trespass. A wiretap, on the other hand, may be employed externally by tapping into wires at some point between the sender and receiver. Thus under the trespass test, while warrantless trespassory bugging devices were prohibited by fourth amendment warrant protection, those wiretaps conducted without a trespass were not.

15. In Katz, while holding the warrant requirement applicable to electronic surveillance, the Court explicitly declined to include in its holding those cases "involving the national security." 389 U.S. at 358 n.23. In refusing to include national security cases in its holding, however, the Court also neglected to define what would constitute a national security case. Id. Thus, it could be argued that any threat to the security of the nation—be it internal or external—was included in the term national security. In a subsequent decision, however, the Court distinguished between foreign and domestic national security cases. In United States v. United States Dist. Court (Keith), 407 U.S. 297 (1972), the Court held that those cases involving purely domestic aspects of the national security were subject to the warrant provision of the fourth amendment. Id. at 321. Thus the broad "national security" reservation in Katz had been reduced to include only "foreign security" cases since the Court, in Keith, refused to express any opinion as to the issues raised by the foreign aspects of national security. Id. at 308-09, 321-22.

The domestic aspects of the nadonal security are those cases where the threat to the nation comes from a wholly internal source. A group or person is wholly domestic when it is neither a foreign power nor an agent of a foreign power. Thus a political organization based in the United States, receiving all economic and human resources from within the United States would be considered domestic.

The foreign aspects of the national security concern those cases where the threat to the nation comes from a foreign power or an agent of a foreign power. A foreign agent would seem to include any person or organization which works closely or conspires with, or under the direction of a foreign power. Thus a political organization based in the United States and composed totally of American citizens which receives substantial financial support from a foreign power would, apparantly, be considered a foreign agent.

For the purposes of this Note, given the above definition, the terms domestic and foreign security shall be used independently.

16. In a footnote to the Keith decision the Court noted the view of several authorities that, while prohibited in the domestic area, warrantless surveillances may be permissible in the foreign area. United States v. United States Dist. Court (Keith), 407 U.S. 297, 322 n.20 (1972). While at least one court has relied upon this footnote as carving out an exception to the warrant provision where foreign security is involved, United States v. Brown, 484 F.2d 418, 425-26 (5th Cir. 1973), cert. denied, 415 U.S. 960 (1974), it seems the better view, in light of the Court's refusal to express an opinion on the issue, 407 U.S. at 321-22, that the Court was merely citing these authorities for informational purposes rather than suggesting that an exception be carved out in the area of foreign security.

decisions concerning fourth amendment safeguards where national security surveillances are employed. Moreover, Congress has failed to enact any legislation regulating the use of national security surveillances.[17]

The Foreign Intelligence Act was aimed at filling the national security gap by requiring a judicial warrant prior to the implementation of national security electronic surveillances.[18] The Act was largely a response to the revelation of abusive warrantless electronic surveillance which was performed in the name of national security,[19] the most serious of which was found to exist during the Johnson and Nixon administrations. During these administrations conversations between certain legislators and foreign officials were intercepted by FBI wiretaps and bugging devices and the information forwarded to the President.[20] Although none of these legislators were the actual targets of the warrantless surveillances, their conversations were "overheard" through the intercepted communications of certain "foreign targets."[21] Thus, the types of abuses flowing from the national security gap,

17. Congress has enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-20 (1970). This Act was designed to provide the procedural requirements for obtaining an order (warrant) authorizing electronic surveillance employed in criminal investigations. Thus while the use of criminal surveillances has been regulated by federal legislation, no similar requirement exists in the foreign surveillance area.

18. Senate Report, supra note 1, at 11.

19. Senate Report, supra note 1, at 9-10.

20. N.Y. Times, May 10, 1976, at 14, cols. 4-7. It was felt by Presidents Johnson and Nixon that many of the protests against their respective Vietnam policies, particularly those voiced in certain Senate hearings, were generated by foreign officials. Id.

21. Id. These abuses are not limited to merely overhearing the conversations of American citizens while speaking to foreign officials (or agents), but include the possibility of these American citizens being classified as foreign agents by virtue of these communications and, in fact, becoming targets themselves. See text accompanying notes 58-60 infra.

For a number of other cases in which the national security was used to disguise certain questionable executive branch surveillances see generally 119 Cong. Rec. S 23026 (daily ed. Dec. 17, 1973). The more significant abuses were: (1) installation in 1969 of warrantless wiretaps on 13 government officials and four newsmen, purportedly because they were leaking or publishing sensitive foreign intelligence information. Two of these wiretaps were even continued after their subjects had left government service and had begun working on Senator Muskie's presidential campaign (see generally Hearings on the Role of Dr. Henry A. Kissinger in the Wiretapping of Certain Government Officials and Newsmen Before the Senate Comm. on Foreign Relations, 93d Cong., 2d Sess. (1974)); (2) White House authorization in 1969 of a burglary of the home of newspaper columnist Joseph Kraft for installation of an alleged national security wiretap; (3) invocation of national security in inducing the CIA to assist in the burglary of Daniel Ellsberg's psychiatrist's offices; (4) the 1970 drafting by the White House of a plan to engage in massive warrantless wiretapping and burglary which, although approved on national security grounds, was scrapped after objection from FBI Director Hoover; (5) surveillance by the Kennedy Administration of Dr. Martin Luther King, Jr. and other civil rights activists who were suspected of being Communist sympathizers or dupes.

Such examples, multiplied several times over, demonstrate the need for judicial scrutiny of Executive surveillance practices. Indeed, one might even question whether the Government would have had the audacity to present many of these practices to a neutral magistrate had a warrant been required.

though directed at foreign targets, directly affect American citizens.[22]

The purpose of this Note is to examine the Foreign Intelligence Act and those constitutional issues raised by its attempt to fill the national security vacuum. In this effort the history of the gap and the presidential claim of an inherent constitutional power to operate unencumbered by legislative strictures in the national security area will be investigated.

The Gap

Over three decades ago President Franklin D. Roosevelt sent a confidential memorandum to Attorney General Jackson which authorized him "to secure information by listening devices direct[ed] to the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies."[23] The memo further requested that these investigative techniques be "conducted to a minimum and limit[ed] . . . insofar as possible to aliens."[24] This memo has served as the cornerstone for the assertion of seven administrations that the President can authorize warrantless electronic surveillance for national security purposes.[25]

This presidential power, it is claimed, is constitutionally based in the executive's power to conduct the nation's foreign affairs and, consequently, is immune from the constitutional restraints of the fourth amendment.[26] To assess the viability of this argument one must first understand the relationship between electronic surveillance and fourth amendment protections.

In *Olmstead v. United States*,[27] the Supreme Court held that absent a physical trespass, the interception of communications did not constitute a search or seizure within the meaning of the fourth amendment.[28] In rendering

---

22. The purpose behind the amendments to the Constitution were to insure the protection of certain personal liberties from the possibility of governmental encroachment. This spirit of personal liberty was broader than any governmental encroachment contemplated at the time the amendments were enacted. As Justice Brandeis pointed out in his dissenting opinion to the Olmstead decision: "The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and . . . expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions." Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

23. Zweibon v. Mitchell, 516 F.2d 594, 674 (D.C. Cir. 1975) (en banc) (plurality opinion), cert. denied, 425 U.S. 944 (1976).

24. Id.

25. Id.; Senate Report, supra note 1, at 11-12; Senate Hearings, supra note 3, at 1.

26. E.g., Zweibon v. Mitchell, 516 F.2d. 594, 616-19 & nn. 65-66 (D.C. Cir. 1975) (en banc) (plurality opinion), cert. denied, 425 U.S. 944 (1976); Senate Report, supra note 1, at 13-15, Senate Hearings, supra note 3, at 1.

27. 277 U.S. 438 (1928).

28. Id. at 466. In establishing a trespassory/non-tresspassory distinction for purposes of fourth amendment protections, the Court included bugging as a search and seizure since bugging could be accomplished only by means of a physical trespass. Zweibon v. Mitchell, 516 F.2d 594, 618 & n.64 (D.C. Cir. 1975) (en banc) (plurality opinion), cert. denied, 425 U.S. 944 (1976). In his

the fourth amendment inapposite, the Court also removed the necessity for an assertion, by either President Roosevelt or subsequent administrations, of a presidential immunity since there were no constitutional restraints from which to be immune.[29] Thus it seems that both the Roosevelt memorandum and the subsequent presidential practice of authorizing warrantless national security surveillances were not claims to an immunity from constitutional restraints.[30]

It was not until 1967 that the Supreme Court, in *Katz v. United States*,[31] held that the electronic interception of personal conversations in and of itself constituted a search and seizure and was entitled to the protection of the fourth amendment.[32] In discarding its prior trespassory/non-trespassory distinction, the Court emphasized that "the Fourth Amendment protects people, not places"[33] and the legitimate expectations of conversational privacy were to be shielded from the uninvited ear of government.[34] The Court noted, however, that its opinion did not deal with foreign security matters and, consequently, avoided the question of "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security . . . ."[35] The thrust of the Court's decision, the national security reservation notwithstanding, was to prohibit, for the first time, all warrantless electronic surveillance as an unconstitutional search and seizure. Consequently, in order to continue these surveillances it is necessary for the President to assert an immunity either from the fourth amendment as a whole, or merely from its warrant provision.[36]

---

dissent Justice Brandeis vigorously opposed the majority's trespassory/non-tresspassory distinction as an invitation to the infringement of personal privacy. Olmstead v. United States, 277 U.S. 438, 473-75 (1928) (Brandeis, J., dissenting).

29. Zweibon v. Mitchell, 516 F.2d 594, 617-18 (D.C. Cir. 1975) (en banc) (plurality opinion), cert. denied, 425 U.S. 944 (1976).

30. Later cases had, however, construed section 605 of the Federal Communications Act of 1934, 47 U.S.C. § 605 (1970), superseded by 18 U.S.C §§ 2510-20 (1970), as prohibiting the interception of communications. E.g., Nardone v. United States, 302 U.S. 379 (1937). However, this was a statutory limitation upon wiretapping. Consequently, until Katz, there remained no constitutional restrictions on the President's power to conduct wiretaps.

31. 389 U.S. 347 (1967).

32. Id. at 353.

33. Id. at 351.

34. Id.

35. Id. at 358 n.23. It is possible to read this footnote as indicating that at least some satisfaction of the fourth amendment would be necessary. (The concurring opinions of Justices Douglas and White differed on this point. Compare 389 U.S. at 359 (Douglas, J., concurring) with 389 U.S. at 363-64 (White, J., concurring).) It therefore appears possible that where the national security is involved other safeguards (e.g., post-surveillance warrants) may render the surveillance reasonable. United States v. Butenko, 494 F.2d 593, 605 (3d Cir.) (en banc), cert. denied, 419 U.S. 881 (1974).

36. Zweibon v. Mitchell, 516 F.2d 594, 618-19, (D.C. Cir. 1975) (en banc) (plurality opinion), cert. denied, 425 U.S. 944 (1976). Congress, responding to the Katz decision, enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 which established specific procedural requirements for obtaining a warrant authorizing the use of electronic surveillance. 18 U.S.C. §§ 2510-20 (1970). An integral part of this legislation was the controversial Title III Presidential

In *United States v. United States District Court (Keith)*[37] the Court addressed the issue of whether the President could be subject to the warrant requirement where the domestic aspects of national security were involved.[38] These include only those targets of electronic surveillance which are wholly domestic—*e.g.*, citizens of the United States who have neither direct nor indirect involvement with a foreign power or its agents.[39] In *Keith*, three United States nationals charged with conspiring to destroy government property sought full disclosure of conversations intercepted by electronic devices. The conversations were intercepted without a warrant to obtain information relevant to national security. The defendants alleged that the intercepted conversations might have tainted the evidence upon which the indictment was based and should properly be excluded since they were procured as a result of an illegal or unreasonable search or seizure.[40] The government's defense was that these wiretaps, installed for national security reasons pursuant to a constitutional power of the President, were reasonable for the purposes of the fourth amendment.[41] The Government asserted lack of judicial competence, the potential for security leaks, the need for strategic information gathering and an undue administrative burden as possible grounds for exempting such surveillances from judicial scrutiny.[42]

In considering the applicability of the fourth amendment warrant requirement to domestic security surveillances, the Court engaged in a balancing of

Disclaimer which provides, in part, that "[n]othing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation . . . to obtain foreign intelligence information . . . or to protect national security information against foreign intelligence activities." Id. § 2511(3). Disclaimer is the term ordinarily used to characterize 18 U.S.C. § 2511(3) (1970). E.g., Zweibon v. Mitchell, 516 F.2d 594, 663 (D.C. Cir. 1975) (en banc) (plurality opinion), cert. denied, 425 U.S. 944 (1976). On its face, this provision appears to disclaim any intention of legislating in the area of national security. Moreover, the entire Act, with the exception of the presidential disclaimer, is clearly directed toward electronic surveillance employed in the context of criminal investigations. It has been suggested, however, that this provision was not designed to be a final disclaimer but, rather, to depend upon subsequent judicial determination of the President's power to issue warrantless national security surveillances. Note, Electronic Intelligence Gathering and the Omnibus Crime Control and Safe Streets Act of 1968, 44 Fordham L. Rev. 331, 333-39 (1975). Should the Court hold that the President has the power to issue warrantless national security surveillances, the provision would disclaim any intent to legislate. However, should it be ultimately resolved that no such constitutional power exists, the disclaimer would have the reverse effect of subjecting the President to the Act's procedural requirements. Id.

37. 407 U.S. 297 (1972). It was against Judge Keith that a mandamus proceeding was brought to prevent disclosure of electronic surveillance information to a criminal defendant. This decision, therefore, is called the Keith case after District Judge Damon Keith.

38. Id. at 302.

39. See note 11 supra.

40. 407 U.S. at 299-300.

41. Id. at 318-19. The government interpreted the Title III Presidential disclaimer to mean that "'in excepting national security surveillances from the Act's warrant requirement Congress recognized the President's authority to conduct such surveillances without prior judicial approval.'" Id. at 303.

42. Id. at 318-21.

the basic governmental and individual interests at stake.[43] On the one hand was the duty of the President to protect the domestic security, and on the other the potential dangers that warrantless surveillances pose to an individual's privacy and freedom of expression.[44] These interests were balanced not only against each other but also against the basic tenets underlying the fourth amendment.[45] The Court held that the warrant requirement was applicable in cases involving the domestic aspects of national security intelligence gathering and specifically rejected the establishment of an exception to the warrant requirement in that area.[46]

The protection afforded by the *Keith* decision appears to be very limited. The only persons afforded protection are those who come under the classification of wholly domestic.[47] The Court neglected to specifically define what was and was not contained in the domestic aspects of national security cases.[48] Suppose a group or organization consists entirely of American citizens, yet is funded to some extent by a foreign power. Is this organization now precluded from the protection afforded by *Keith*? Moreover, if an individual has significant contact with a foreign power or its representatives, will such contact render this person a foreign agent for purposes of fourth amendment protections? Thus, any situation which is not wholly domestic may be classified as foreign and, therefore, precluded from the protection given by *Keith*.[49]

THE ACT

After more than three decades of warrantless electronic surveillance in the area of national security, the scope of presidential power and the constitutional restraints upon it remain a mystery.[50] The Foreign Intelligence Surveillance Act of 1976 would have done much to solve this mystery by imposing substantive and procedural controls on the use of electronic surveillance for

---

43. Id. at 310-13.

44. Id. at 316-18.

45. Id. at 321. Since no warrant had been obtained in this case, it was unnecessary for the Court to consider the applicability of Title III procedural requirements and the Court declined to do so. Id. at 308. Moreover, in construing the Presidential disclaimer provision it was found that the provision was totally neutral in that it neither conferred nor limited the President's power in the national security area—it merely left the presidential powers where it found them. Id. at 303. Thus, no congressional exemption to the warrant requirement was found to exist.

46. The thrust of the Keith decision appears to be that the wartant requirement may not be suspended merely because there exists a legitimate governmental need to engage in certain activity. Id. at 310-14. Moreover, if an exception is to be carved out of the warrant provision, the justification for such an exception must be somewhat compelling to justify the suspension of conversational privacy. Cf. id. at 319-21.

47. Id. at 309 & n.8.

48. Id.

49. Cf. id.

50. See Senate Report, supra note 1, at 18-20; Senate Hearings, supra note 3, at 7-13 (statement of Attorney General Levi); L.E.A.A. Newsletter, June 1976, at 6, cols. 1-3.

foreign intelligence purposes. Unfortunately, after extensive debate and amendment, time ran out and the Act was left for re-introduction in the 95th Congress. Nevertheless, an analysis of its provisions and possible effects is a valuable enterprise for a number of reasons. First, the Foreign Intelligence Act is the fifth such act proposed concerning the regulation of warrantless foreign security surveillances since 1973.[51] This indicates that in all probability another attempt to legislate in this area will soon be made. Second, the great need for legislation evidenced by past abuses renders the probability of future legislation almost a certainty.[52] Third, this Act, largely a composite of all its unsuccessful predecessors, is the result of all the hearings and debates surrounding the previous Acts and is likely to be relied upon when its successor is introduced. Thus, the new bill will probably be quite similar to the Foreign Intelligence Act of 1976.

As previously noted, the Act was directed specifically at filling the gap left by the *Keith* decision by addressing the foreign aspects of national security surveillances.[53] A foreign power, as defined by this Act, includes not only members of a foreign government, political party, or military force but also foreign commercial entities doing business in the United States and foreign based terrorist groups.[54] By its terms, the Act provides protection not only to those persons directly involved in the foreign government but also to those who, even though possibly opposed to the foreign government in power (*e.g.*, terrorist groups), may be so related to its political scene as to be a valuable source of intelligence information and, as such, a likely target of surveillance. An agent of a foreign power is similarly defined in very broad and inclusive terms. An agent may either be a non-permanent resident alien who is an officer or employee of a foreign power or any person, including an American citizen, who, under the direction of a foreign power, engages in "clandestine intelligence activities, sabotage, or terrorist activities, or who conspires with, or knowingly aids or abets such a person in engaging in such activities."[55]

These definitions would help to accomplish two goals. First, as protection afforded foreign powers and agents is increased, more protection is afforded to those American citizens who are likely to communicate with them. As noted previously, one need not be the target of a national security surveillance to have personal liberties violated since anyone communicating with a foreign power (or its agent) is vulnerable to the interception of communications.[56] Second, it avoids the application of a double standard of fourth amendment protections afforded to those persons who are wholly domestic. As the law stands now any persons (non-foreign power or agent) conversing with one another are assured that if their conversation is intercepted by the govern-

51. Senate Report, supra note 1, at 9 & n.2.

52. Id. at 9-11; see note 21 supra.

53. Senate Report, supra note 1, at 8, 11-18.

54. Foreign Intelligence Act § 2521(b)(5). The term "foreign power" means those persons officially affiliated with a foreign power such as an ambassador, minister or the like.

55. Id. § 2521(b)(ii).

56. See text accompanying notes 20-21, 47-49 supra.

ment, it is done so pursuant to prior judicial authorization.[57] However, either person, if communicating with a foreign power, an agent of a foreign power, or anyone having a significant connection with either, has no such assurance.[58]

After defining its terms and scope, the Act goes on to provide specific procedural requirements to be followed in submitting applications to the court for an order authorizing a foreign intelligence surveillance.[59] These procedural requirements may be divided into administrative,[60] judicial,[61] and general safeguards.[62]

Concerning the administrative safeguards, the Act requires that before an application be made to the court it must first be authorized by the President and then approved by the Attorney General.[63] An application under this act is properly authorized by the President only when he has, in writing, empowered the Attorney General to approve applications for submission to the court.[64] The purpose of this procedure is to insure that the President in fact wants to carry on foreign intelligence surveillance and that the Attorney General is not acting upon his own determination that such surveillance is necessary.[65]

---

57. This conclusion is dictated by the Supreme Court decision in United States v. United States Dist. Court, 407 U.S. at 314-21 (warrant required in cases involving the domestic aspects of national security intelligence gathering).

58. Thus, there is no assurance that such a surveillance is reasonable—i.e., based upon probable cause. The situation presented by this fact pattern appears to present severe first amendment problems. As indicated above, if an American citizen decides to communicate with a foreign official he runs two risks. First, there is the risk that if their communication is being intercepted as a result of the foreign official being a target of a national security surveillance, there is no assurance that the interception is reasonable since no judicial warrant need be secured. Thus, the surveillance may be based upon the sole determination of the current administration that such surveillance is necessary. Second, there is the risk that the American citizen by communicating with this foreign official will be deemed to have such significant foreign ties as to be himself classified as a foreign agent. Thus, a domestic person may refrain from communicating with a foreign official for fear of either a warrantless interception of the communication or being classified as a foreign agent as a result of the communication. In either case the chilling effect upon the person's freedom of speech and association are clear. Zweibon v. Mitchell, 516 F.2d 594, 633-35 (D.C. Cir. 1975) (en banc) (plurality opinion), cert. denied, 425 U.S. 944 (1976); cf. United States v. United States Dist. Court, 407 U.S. at 313 ("National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Though the investigative duty . . . may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech.").

59. Foreign Intelligence Act §§ 2522-27.

60. Id. §§ 2522, 2524, 2527.

61. Id. § 2525.

62. Id. § 2523.

63. Id. § 2522.

64. Id.

65. Only one written authorization is required to empower the Attorney General to approve applications in any number of surveillances for as long as the President lets the single authorization stand. See Senate Report, supra note 1, at 34.

The application itself is quite detailed to insure the existence and reliability of the facts giving rise to the particular surveillance. It is also necessary to reveal the identity of the targets of the surveillance, and the specific techniques to be employed. The application must further state the facts relied upon in classifying the targets as foreign, the information sought as foreign intelligence information, and how the government intends to minimize the interception of unrelated information.[66]

The judicial safeguards dictate that a judge shall, if the application was properly authorized by the President and approved by the Attorney General, enter an *ex parte* order approving the surveillance. The judge must affirm that the facts submitted to him establish probable cause to believe that the target is a foreign power or an agent of a foreign power and that the information sought is foreign intelligence information. Finally, he must confirm that the procedures are reasonably designed to minimize the collection of unrelated information.[67]

The general requirements essentially designate the judges to grant orders for electronic surveillance and the appellate route to be followed by the Attorney General upon the denial of an order.[68] The Act also provides that the Chief Justice of the Supreme Court shall designate seven district court judges, each of whom will have jurisdiction to hear applications for and grant orders approving electronic surveillance.[69] Further, the Chief Justice would, under the Act, designate three judges to comprise a special court of appeals to hear appeals by the United States from the denial of any application.[70] The Government would have the right to appeal an affirmance of a denial by that court to the Supreme Court. All appeals are to be heard and determined as expeditiously as possible.[71] The Act provides that applications and orders be sealed by the presiding judge and kept according to security measures to be established by the Chief Justice and the Attorney General.[72]

The final and, from a constitutional perspective, the most controversial section of the Act is that which squarely addresses the power of the President in the area of foreign intelligence gathering. Section 2528, entitled "Presidential Power,"[73] provides, in essence, that nothing contained in the Act was intended to affect the exercise of any constitutional power the President may

66. Foreign Intelligence Act § 2524.

67. Id. § 2525. Subsection (a) of this section specifies the findings the judge must make before he grants an order approving the use of electronic surveillance for foreign intelligence purposes. While the issue of the order is mandatory if all the requirements of subsection (a) are present, the judge has discretionary power to modify the order sought—e.g., the period of authorization or the minimization procedures to be followed.

68. Id. § 2523(a) & (b).

69. Id. § 2523(b).

70. Id.

71. Id. § 2523(c). The Attorney General has access to this special court of appeals as a matter of right. Id. § 2523(b). The appeal as of right applies even to appeals to the Supreme Court. Query if this also includes the right to a rehearing if the Supreme Court should deny the application?

72. Id. § 2523(c).

73. Id. § 2528.

have to gather foreign intelligence information through the use of electronic surveillance if either the surveillance falls outside the definition of electronic surveillance or "the facts and circumstances giving rise to the acquisition are so unprecedented and potentially harmful to the Nation that they cannot be reasonably said to have been within the contemplation of Congress in enacting this chapter . . . Provided, That in such an event the President shall, within a reasonable time thereafter, transmit to the Committees on the Judiciary of the Senate and House of Representatives" the facts surrounding this unprecedented situation.[74] The purpose of this section was to clearly establish the intent of Congress to legislate in the area of foreign intelligence gathering by regulating the exercise of presidential powers—be they constitutionally based or not—in all but two well defined situations: *i.e.*, if the surveillance did not come within the definition of electronic surveillance or the facts were unprecedented and potentially harmful.[75]

The Constitutional Ramifications of Imposing A Warrant Requirement on the President in National Security Cases

The Applicability of the Fourth Amendment

The attempt to regulate foreign intelligence surveillance through the Foreign Intelligence Act raises three constitutional issues. First, given the sweeping language in a number of cases addressing the President's constitutional power to conduct foreign affairs, may the exercise of such power be implemented without regard for the fourth amendment? Second, assuming the applicability of the fourth amendment to the President's foreign affairs powers, will the warrant provision unduly fetter the legitimate exercise of these powers? Third, assuming that the warrant provision presents no undue restraint upon this power, does the Foreign Security Act, which would require more than merely obtaining a search warrant, unduly fetter these powers?[76]

---

74. Id.

75. Senate Report, supra note 1, at 49-54; Senate Hearings, supra note 3, at 16-20.

76. During the hearings and in the final report of the Subcommittee on Criminal Laws and Procedures a fourth constitutional problem was raised. The subcommittee felt that the question of whether Congress may legislate in an area where the President has a constitutional power was a major barrier for this piece of legislation to hurdle. Senate Hearings, supra note 3, at 2 (remarks of Senator McClellan); Senate Report, supra note 1, at 50-51. In order to justify this Act the Committee relied exclusively upon the Supreme Court's decision in Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952). In Youngstown, President Truman, relying upon his constitutional war powers, ordered the seizure and operation of certain steel mills in order to avert a nation-wide strike of steel workers during the Korean War. The Court's opinion, narrowly drawn, held that the President had no power stemming either from Congress or the Constitution to seize steel mills. Id. at 585-86.

Justice Jackson, in his concurring opinion, wrote: "When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter." Id. at 637 (Jackson, J., concurring). In the Senate Report this

The power to engage in foreign intelligence gathering may be implied as a necessary concomitant of the President's express powers as Commander-in-Chief of the armed forces,[77] as the officer in charge of the nation's foreign affairs,[78] and as the protector and defender of the Constitution.[79] While there is no dispute that from these express powers the implied power to engage in foreign security surveillances may be inferred, what remains to be decided is whether these constitutional powers render the fourth amendment inapplicable.

There are two leading Supreme Court cases which, though not concerned with the fourth amendment, are cited in support of the contention that foreign

---

concurring opinion was constantly referred to. E.g., Senate Report, supra note 1, at 50-52, 75 n.13 (views of Senators Abourezk, Hart, and Mathias), 141 (minority view of Senator Tunney). Moreover, Attorney General Levi interpreted the Youngstown decision as indicating "that when a statute prescribes a method of domestic action adequate to the President's duty to protect the national security, the President is legally obliged to follow it." Senate Report, supra note 1, at 51 & n.36.

The subcommittee's absolute reliance upon Youngstown seems misplaced for two reasons. First, the Court's holding in Youngstown was that no constitutional power was found to exist to justify the President's activities. In regard to national security intelligence, the Supreme Court has recognized the existence of a Presidential power, although presently undefined, to gather such information. Cf. United States v. United States Dist. Court, 407 U.S. at 310-12. Thus, the recognized existence of a constitutional power seems to preclude any reliance (certainly absolute reliance) upon Youngstown. Second, in Youngstown, even assuming that the Jackson concurrence was the Court's holding, the Taft-Hartley Act was enacted before the President seized the mills. In contrast, in the case of national security intelligence gathering, the Court will be faced with legislation that comes after over thirty years of Presidential practice. See Senate Report, supra note 1, at 13-15; Senate Hearings, supra note 3, at 1. Moreover, given this prior executive practice, it is at least possible (reversing the Jackson reasoning in Youngstown) that where Congress takes measures incompatible with established presidential practice, their power is at its lowest ebb. Such a reversal of Jackson's reasoning, so heavily relied upon by the subcommittee, could prove devastating to any future attempt to legislate in the area of foreign security.

It seems that rather than stretching the Youngstown case to its limits (if, in fact, not surpassing them), the better course would be simply to rely upon the necessary and proper clause, U.S. Const. art. 1, § 8, cl. 18, which provides that Congress shall have power "[t]o make all Laws which shall be necessary and proper for carrying into Execution . . . [the] Powers vested by this Constitution in the Government of the United States . . . ." Id. The classic construction of the powers expressed in the necessary and proper clause is that of Chief Justice Marshall in McCulloch v. Maryland, 17 U.S. (4 Wheat.) 316 (1819): "Let the end be legitimate, let it be within the scope of the constitution, and all means which are appropriate, which are plainly adapted to that end, which are not prohibited, but consist with the letter and spirit of the constitution, are constitutional." Id. at 421. Thus "[w]hatever legislation is appropriate . . . to carry out the objects the amendments have in view, whatever tends to enforce submission to the prohibitions they contain, . . . is brought within the domain of congressional power." Ex parte Virginia, 100 U.S. 339, 345-46 (1879). It seems, therefore, that the fourth amendment is a proper subject of legislative action to secure its guarantees. Cf. Katzenback v. Morgan, 384 U.S. 641 (1966) (Congress may legislate to secure the guarantees of the fourteenth amendment).

77. U.S. Const. art. II, § 2, cl. 1.

78. Id. § 2, cl. 1, 2.

79. Id. § 1, cl. 8.

intelligence surveillance is immune from the requirements of this amendment. In *United States v. Curtiss-Wright Export Corp.*,[80] the Court held that the federal government's domestic and foreign powers are of a very different scope because they differ in origin and nature. It then stated that in relation to foreign affairs the President alone has the power to act as representative of our nation. Moreover, the Court noted that confidential sources are necessary to the exercise of his duties, and, consequently, they should remain confidential.[81] Later, *Chicago & Southern Air Lines, Inc. v. Waterman Steamship Corp.*[82] stated that in his capacity as Commander-in-Chief and as the organ of foreign affairs, the President "has available intelligence services whose reports are not and ought not to be published to the world. It would be intolerable that courts, without the relevant information, should review and perhaps nullify actions of the Executive taken on information properly held secret."[83]

Two recent circuit court decisions have expressly addressed warrantless foreign security surveillances and have resolved these cases based upon the sweeping language contained in *Curtiss-Wright* and *Waterman*.[84] The Fifth Circuit, in *United States v. Brown*,[85] held that warrantless foreign security surveillances were constitutionally permissible. The opinion declared that on the basis of "the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs . . . the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence."[86] The Court added that any "[r]estrictions upon the President's power which are appropriate in cases of domestic security become artificial in the context of the international sphere."[87] In *United States v. Butenko*,[88] the Third Circuit reached the same conclusion, finding that these surveillances would be reasonable without a warrant even though some abuses may arise.[89]

The Third and Fifth Circuits' decisions are based on very conclusory analytic frameworks and tend more to confuse than to clarify the issues of presidential power and the applicability of constitutional restraints. In *Brown*, the court failed to pay even lipservice to the type of constitutional analysis suggested by the *Keith* decision: there was no attempt at balancing the various interests at stake. The Fifth Circuit merely stated that the President has the power to authorize intelligence gathering by means of warrantless electronic

80. 299 U.S. 304 (1936).

81. Id. at 315-20.

82. 333 U.S. 103 (1948).

83. Id. at 111.

84. United States v. Butenko, 494 F.2d 593, 602 (3d Cir.) (en banc), cert. denied, 419 U.S. 881 (1974); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973), cert. denied, 415 U.S. 960 (1974). See also United States v. Smith, 321 F. Supp. 424, 426 (C.D. Cal. 1971) (dictum); United States v. Clay, 430 F.2d 165, 171 (5th Cir. 1970), reversed on other grounds, 403 U.S. 698 (1971).

85. 484 F.2d 418 (5th Cir. 1973), cert. denied, 415 U.S. 960 (1974).

86. Id. at 426.

87. Id.

88. 494 F.2d 593 (3d Cir.), cert. denied, 419 U.S. 881 (1974).

89. Id.

surveillance.[90] In *Butenko*, the Third Circuit ignored the Supreme Court's rejection of post-search sanctions as offering viable fourth amendment protections in the domestic area and relied, without explanation, upon this procedure as a means of affording adequate protection in the foreign security area.[91] Thus these decisions are better viewed as evidencing the on-going struggle between the constitutional issues raised by foreign security surveillances rather than as a clarification of these problems.[92]

In *Zweibon v. Mitchell*,[93] the District of Columbia Circuit, while limiting its holding to requiring a warrant prior to the surveillance of a domestic organization, questioned whether any national security exception to the warrant requirement would be constitutional.[94] Unlike the Fifth and Third Circuit cases, the *Zweibon* opinion, written by Judge J. Skelly Wright, presented a complete and detailed analysis of the issues raised by foreign security surveillances, paralleling the type of fourth amendment analysis employed by the Supreme Court in *Keith*.[95] After a brief survey of cases recognizing the vast scope of the President's power to conduct foreign affairs, the court dismissed the possibility that the fourth amendment may be inapplicable in the area of foreign security surveillances.[96] While recognizing that there is support for the proposition that the President's powers concerning foreign affairs are not limited to those specifically enumerated in the constitution, the *Zweibon* court stated that they did not override the fourth amendment but, rather, had to be reconciled with it.[97]

This conclusion appears to be well grounded. In *Curtiss-Wright*,[98] the Court itself recognized that "like every other governmental power, [the President's plenary power over foreign relations] must be exercised in subordination to the applicable provisions of the Constitution."[99] The question actually presented in *Curtiss-Wright* was the constitutionality of a congressional delegation of power in granting the President authority to prohibit arms

90. United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973), cert. denied, 415 U.S. 960 (1974).

91. United States v. Butenko, 494 F.2d 593, 605 (3d Cir.), cert. denied, 419 U.S. 881 (1974).

92. Senate Report, supra note 1, at 18 n.17 (noting the lack of systematic analysis of the Brown and Butenko decisions), 80 n.24 (additional views of Senators Abourezk, Hart, and Mathias reaching the same conclusion).

93. 516 F.2d 594 (D.C. Cir. 1975) (en banc) (plurality opinion), cert. denied, 425 U.S. 944 (1976).

94. Id. at 613-14.

95. Id. at 612-13.

96. Id. at 626-27, 633-34, 641. The Court considered the argument that the conduct of foreign affairs is an exercise of the President's political power and as such beyond judicial review. Id. at 620-21. Consideration was also given to the evidentiary privilege of the Executive concerning the production of documents whose publication might endanger either military or diplomatic secrets. Id. at 625-27. Although these points are beyond the scope of this Note, it should be noted that as to each argument the Court found no bar to its consideration of fourth amendment protections. Id. at 620-21, 625-26.

97. Id. at 627.

98. 299 U.S. 304 (1936).

99. Id. at 320.

shipments to an area of armed conflict.[100] The Court did not address the question of whether these powers are to be exercised in accordance with the strictures of the fourth amendment.[101] The *Waterman*[102] decision was cloaked in very broad language concerning the President's foreign affairs powers.[103] The question presented was the judicial review of certain presidential acts concerning foreign air transportation.[104] Again, the Court did not address the exercise of these powers in the context of the fourth amendment.[105] Thus, these cases, so often cited as establishing the breadth of the foreign affairs powers, do little more than identify and define these powers in a context where there was no assertion of an express countervailing constitutional limitation.

To conclude that the President's power in this area is to be tested outside the framework of the fourth amendment would, as the *Zweibon* court noted, be to ignore the series of cases which have adhered to the principle—even in time of war and civil insurrection—that the President cannot exercise his power without regard for the Bill of Rights.[106] For example, in *Ex parte Milligan*,[107] the Court prevented the President from suspending the sixth amendment right to jury trial where the courts were open and their process available.[108] A similar result was reached in *Duncan v. Kahanamoku*,[109] where the substitution of military law for civilian process was held unconstitutional despite allegations that Hawaii was in danger of attack and martial law was necessary for its protection.[110] Further support for this position can be found in *Home Building & Loan Association v. Blaisdell*,[111] where the Court, in dictum, stated that "even the war power does not remove constitutional limitations safeguarding essential liberties."[112] Finally, in *United States v. Washington Post Co.*,[113] the Government urged the court to restrain the publication of the contents of a classified study recounting the history of American decision-making on Vietnam policy, asserting that the defense interests of the United States would be greatly prejudiced.[114] The Court of Appeals for the District of Columbia Circuit held that the Government had

100. Id. at 314-15.
101. Zweibon v. Mitchell, 516 F.2d at 621-22.
102. 333 U.S. 103 (1948).
103. Id. at 111 (dictum).
104. Id. at 104-06.
105. Zweibon v. Mitchell, 516 F.2d at 622-23.
106. Id. at 621-23, 626-27.
107. 71 U.S. (4 Wall.) 2 (1866).
108. Id. at 121.
109. 327 U.S. 304 (1946).
110. Id. at 316-17.
111. 290 U.S. 398 (1934).
112. Id. at 426 (dictum).
113. 446 F.2d 1327 (D.C. Cir.) (en banc) (per curiam), aff'd sub nom. New York Times v. United States 403 U.S. 713 (1971) (per curiam).
114. Id. at 1328.

not overcome the first amendment's presumption against the constitutionality of prior restraints on the press[115] and the Supreme Court affirmed.[116]

The thrust of these decisions is that the President is subject to certain constitutional limitations in the exercise of his constitutional powers. This is not to say that, given a proper set of facts, the President could not have fully exercised his powers. Had the *Washington Post* case involved publication of information concerning an upcoming military offensive, or if acts of war had actually closed the courts in *Milligan* and *Duncan*, the Court, upon balancing the interests at stake, may have reached a different result. Thus, Presidential power must be exercised within the framework of constitutional restraints: both the constitutional power and its constitutional limitation must be balanced to insure the legitimate exercise of that power and the protection of the liberties likely to be affected.[117]

Does the Warrant Requirement Apply to a National Security Search?

Judge Wright's opinion in *Zweibon* is instructive on the issue of the reasonableness of a warrantless national security search.[118] Recognizing the importance of both foreign intelligence gathering and the protection of personal liberties, he concluded that the warrant requirement would best serve to harmonize both interests.[119] In reaching this conclusion five possible justifications offered by the government for exempting national security surveillances from prior judicial authorization were discussed.[120] These justifications—lack of judicial competence, security leaks, strategic information gathering, administrative burden, and delay—were virtually the same as those offered in *Keith*.[121] The *Zweibon* decision addressed each of these with the same scrutiny employed in *Keith* and reached the same result in the area of foreign security as *Keith* reached in the domestic area.

In both cases the Government posited that the judicial branch lacked the competence to effectively perceive and decide questions involving foreign security.[122] In *Keith*, the Supreme Court rejected this argument, stating: "If the threat is too subtle or complex for our senior law enforcement officers to convey . . . one may question whether there is probable cause for surveillance."[123] The *Zweibon* court was similarly unpersuaded where questions of foreign security were involved. Essentially, it refused to accept the idea that the Attorney General, chosen for his prowess as an attorney rather than as a diplomat, was more capable than a federal judge to perceive and analyze the

115. Id. at 1328-29.
116. 403 U.S. 713 (1971) (per curiam).
117. Cf. Zweibon v. Mitchell, 516 F.2d at 626-27.
118. Id. at 628-33.
119. Id. at 633-36.
120. Id. at 641-51.
121. 407 U.S. at 319-21.
122. Id. at 320; Zweibon v. Mitchell, 516 F.2d at 641-47.
123. 407 U.S. at 320.

issues raised by a foreign security surveillance.[124] This response seems quite appropriate. There is no reason why a federal judge, deemed by the Supreme Court to be sensitive and comprehending enough to pass upon probable cause in domestic security cases, will become any less so when dealing with foreign security cases.[125]

On the question of security leaks the Government, in both *Keith* and *Zweibon*, argued that the warrant provision would force the President to reveal highly sensitive information. It claimed that providing this information to the judiciary would increase the risk of a security leak which would, in turn, endanger the national security.[126] *Keith* did not recognize a perceptible increase in the risk of a security leak by virtue of a revelation to a federal judge in domestic security cases.[127] The *Zweibon* court found this argument no more compelling in the context of foreign security.[128] In addition to noting, as did *Keith*, that warrant proceedings are *ex parte*, *Zweibon* espoused preventive measures which could be taken to guard against security leaks. The Government, for example, could supply any clerical or secretarial personnel needed, thereby limiting the exposed material to a single judge and insuring the utmost secrecy.[129] The *Keith/Zweibon* conclusion seems to be correct, especially if the Executive supplies the necessary clerical personnel. However, the risk of security leaks would probably be diminished even further if a select group of judges, designated by the Chief Justice or another appropriate member of the federal bench, was appointed to hear all foreign security cases.

The Government urged in both cases that since these surveillances are aimed primarily at the collection and maintenance of strategic information they are less offensive to the fourth amendment than those surveillances designed to end in a criminal prosecution.[130] In *Keith*, the Court apparently accepted the Government's premise that the nature of domestic surveillances was essentially non-prosecutorial, but refused to accept that an individual's constitutionally protected freedoms are any less offended because of this.[131] In *Zweibon*, the court, in reaching the same conclusion, refused to accept the notion that foreign surveillances were non-prosecutorial.[132] The result reached in *Zweibon* seems eminently sensible. Whatever the purpose of a given surveillance may be, it seems clear that the same constitutional infringements will result from its uncontrolled use. It is the means and not the

---

124. 516 F.2d at 641-42, 644.

125. Cf. United States v. United States Dist. Court, 407 U.S. at 320.

126. Id. at 320-21; Zweibon v. Mitchell, 516 F.2d at 647-48.

127. 407 U.S. at 320-21.

128. 516 F.2d at 647.

129. 516 F.2d at 647; cf. Commission for Nuclear Responsibility v. Seaborg, 463 F.2d 788, 794-95 n.12 (D.C. Cir. 1971) (per curiam).

130. United States v. United States Dist. Court, 407 U.S. at 318-19; Zweibon v. Mitchell, 516 F.2d at 648-49.

131. 407 U.S. at 320.

132. 516 F.2d at 648.

ends of a given surveillance which the fourth amendment addresses.[133] Indeed if these surveillances were non-prosecutorial the need for fourth amendment protections would be heightened. Without a trial in which an attempt is made to use the evidence seized without a warrant (or its fruits) all judicial scrutiny would be bypassed. Thus the temptation to intercept non-security information would only increase.[134]

The added burden imposed upon the administration was also urged as a justification for an exception to the warrant provision.[135] This argument was summarily dismissed by *Keith*.[136] Likewise, the *Zweibon* court rejected the argument in the foreign context, refusing to carve out an exception to the protection afforded by the warrant provision based solely upon administrative burdens.[137]

The final justification offered in *Zweibon* was the danger caused by a delay in instituting a foreign security surveillance. It was posited that foreign security surveillance must be hastily employed and any delay, resulting from compliance with the warrant procedure, would cause the loss of crucial information thus threatening the national security.[138] The argument, admitted by the court to be the most persuasive, was both accepted and rejected in part. It was accepted in relation to the apparent necessity for an exception to the warrant requirement in exigent circumstances. These emergency situations, when time is of the essence, call for immediate executive action to prevent the loss of information vital to the national security. However, the court refused to suspend the warrant requirement in all foreign security cases because of the mere potentiality of a rare situation requiring such an exception.[139] Although no similar argument was made concerning domestic security in *Keith*,[140] the *Zweibon* result seems sound. The average length of a foreign security surveillance is between seventy and two hundred days.[141] Moreover, the average surveillance is well planned and must be approved by a number of administrative officials before it is employed.[142] Thus it appears that the emergency situation is clearly exceptional. To exempt all foreign security surveillances would be to let the exception govern the rule.[143] There may be situations, however, where a surveillance may have to be immediately instituted or the national security could be jeopardized. However, in these cases the fourth amendment and the President's constitutional powers can be

133. See United States v. United States Dist. Court, 407 U.S. at 320; Zweibon v. Mitchell, 516 F.2d at 649.

134. United States v. United States Dist. Court, 407 U.S. at 320.

135. Id. at 320; Zweibon v. Mitchell, 516 F.2d at 650-51.

136. 407 U.S. at 321.

137. 516 F.2d at 651.

138. Id. at 649-50.

139. Id.

140. Senate Report, supra note 1, at 79 (views of Senators Abourezk, Hart, and Mathias).

141. Zweibon v. Mitchell, 516 F.2d at 650 & n.177.

142. Id. at 643.

143. Cf. id. at 650.

reconciled. Certain searches which must be instituted without delay have been held reasonable without a warrant.[144] Thus it would not be inconsistent with prior fourth amendment cases to hold that the President may, in order to carry out his constitutional duties, conduct warrantless national security surveillances where there is no time to obtain a warrant.

Another justification, not offered in the *Zweibon* case, but possibly more pursuasive, is that a foreign threat to the national security is more dangerous than a domestic threat. The argument would be that a foreign threat may have as its end a more drastic result than a wholly internal threat. However, both an internal and external organization could have as its objective the reorganization or elimination of our national structure. On the other hand, an important distinction between these two types of organizations is found in the resources available to a foreign and domestic organization. A domestic organization, by definition, will derive its resources from wholly internal sources.[145] This means that not only must the membership of the organization consist only of persons within the United States, but also that the funds necessary to carry on the organization must originate from donations of its members and domestic sympathizers. A foreign organization, on the other hand, has, in addition to all those resources open to its domestic counterpart, any resources available from a foreign source. Thus, not only may its membership be drawn from a larger area, but its operational costs may be received from a larger pocket.

Even conceding that a foreign threat may be inherently more dangerous than its domestic counterpart, there is no logical connection between this and making it unreasonable, in all cases, to secure a search warrant. Certain safeguards may be employed to account for any measurable difference between a foreign and a domestic security threat. Such safeguards could take the form of an escape clause whereby the President, confronted with an extremely dangerous situation, would be able to respond without first applying for a warrant. This would be much the same as the exigent circumstances exception noted above.[146] Just as with the delay argument, for the court to establish a general rule based upon the possibility of an emergency situation would be to let the exception govern the rule.[147] Clearly the better course, rather than foreclosing fourth amendment protections, would be to carve a specific exception to fit these circumstances: to subject the President to the warrant provision absolutely would, given an emergency situation, preclude him from fulfilling his constitutional duty to defend and protect the Constitution.

---

144. E.g., United States v. Edwards, 415 U.S. 800, 802-03, 806-09 (1974) (discussion of the exceptions to the warrant requirement of search incident to a lawful arrest and seizure of evidence of criminal activity where it is likely to be destroyed); see note 9 supra and accompanying text.

145. Cf. United States v. United States Dist. Court, 407 U.S. at 309 n.8.

146. Zweibon v. Mitchell, 516 F.2d at 649-50.

147. Id.

DOES THE FOREIGN SURVEILLANCE ACT UNDULY FETTER THE CONSTITUTIONAL EXERCISE OF PRESIDENTIAL POWER?

The Inherently More Dangerous Foreign Threat

Assuming the validity of this argument—that a foreign threat is inherently more dangerous than its domestic counterpart—the Foreign Intelligence Act anticipates this problem. First, there is the exception clause in the presidential power section which contemplates an unprecedented emergency situation wherein the President is permitted to act upon his own determination that such action is necessary.[148] Second, there is the 24-hour emergency provision of section 2525(d) which enables the Attorney General to authorize a surveillance upon his own authority by merely notifying one of the seven designated judges.[149] Third, there is the speedy appellate route provided by section 2523 insuring rapid hearings and decisions upon the denial of any order authorizing a foreign security surveillance.[150] Given these three provisions, it is hard to imagine a situation, even assuming the greater potential danger posed by foreign threats to the national security, that is so bizarre as to evade both emergency provisions and the rapid appellate route and yet remain so deadly as to pose a significant threat to the national security.[151]

Lack of Judicial Competence

Assuming that this argument is more persuasive in foreign security cases, and that *Keith*'s rejection of this argument in the domestic area is not determinative in the foreign area, the Act, in designating certain federal judges to hear applications for and grant orders approving foreign security surveillances, seems to deflate it.[152] Even if they initially found the subject difficult to grasp, the limited number of judges so designated would soon develop expertise because of the frequency with which they would hear foreign security surveillance applications. Given the lifetime tenure of a federal judge and the relatively short tenure of an Attorney General, it may not be long before the bench will be required to inform the Attorney General of the pertinent subtleties.[153]

Risk of Security Leaks

In addition to the *ex parte* approach embraced by *Zweibon*, the Act provides that all applications and orders are to be sealed by the presiding judge and protected by security measures to be prescribed by the Chief Justice in consultation with the Attorney General.[154] Thus the Attorney General has

148. Foreign Intelligence Act § 2528.
149. Id. § 2525(d).
150. Id. § 2523. These appellate routes are open to the Government as a matter of right. Id.
151. See Senate Report, supra note 7, at 79 (views of Senators Abourezk, Hart, and Mathias).
152. Foreign Intelligence Act § 2523.
153. Zweibon v. Mitchell, 516 F.2d at 644 & n.138.
154. Foreign Intelligence Act § 2523.

a voice in insuring against the risk of security leaks by virtue of his own safeguards.[155]

Danger of Delay

This argument is vitiated by the three emergency provisions of the Act discussed in the above analysis of the inherently more dangerous foreign threat.[156]

Administrative Burden

In order to determine the added burden that the Act imposes upon the administration, one must first review the procedure currently employed before the implementation of a foreign security surveillance. At present, the request must be very specific and must be approved by the FBI at several levels: up to seven supervisors, three subordinate directors, and the Director of the FBI.[157] Further, the Attorney General must approve.[158] It appears that the application called for by the Act requires not only less detailed information but also significantly less procedural involvement. The Act, therefore, does not appear to measurably increase the burden the Government has already imposed upon itself.

The Need For a Legislative Response

It is apparent that either the courts or Congress may require the President to obtain a warrant prior to employing a foreign intelligence surveillance. However, due to the superior protection which it gives to both fourth amendment rights and the national security, it is submitted that Congressional legislation is the alternative which should be chosen.

The judicial branch, absent any legislation concerning foreign security surveillances, would be able to afford fourth amendment protections in a number of ways: a case by case approach;[159] a general warrant approach with an exception for exigent circumstances which necessitate immediate action;[160]

155. Thus the Act provides the type of security measures which prompted the Supreme Court in Keith to conclude that the possibility of security leaks do not necessitate a departure from the warrant provision where domestic security is involved. See United States v. United States Dist. Court, 407 U.S. at 321. The Act is also consistent with the Zweibon treatment of the same argument. See Zweibon v. Mitchell, 516 F.2d at 647-48.

156. See notes 155-58 supra and accompanying text.

157. Zweibon v. Mitchell, 516 F.2d at 642-43.

158. Id.

159. This approach was suggested by the Third Circuit in United States v. Butenko, 494 F.2d 593 (3d Cir.) (en banc), cert. denied, 419 U.S. 881 (1974). The court left any fourth amendment protections to the sanctions incident to post-search litigation. Thus only after the surveillance had been discovered would its reasonableness be tested. Id. at 605.

160. This approach was suggested by the Zweibon decision. Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975) (en banc), cert. denied, 425 U.S. 944 (1976). In Zweibon, the court, in dictum, concluded that absent exigent circumstances a warrant is necessary before employing a foreign security surveillance. Id. at 651 (dictum).

or an absolute warrant requirement.[161] These alternatives all fail to adequately protect either the national security or personal liberties affected by the surveillance. The case by case approach places the government in the unfortunate position of never being sure whether the surveillance they wish to employ requires a warrant. That determination is left for subsequent judicial scrutiny. Moreover, those who are supposedly protected by the warrant requirement would be protected in a retroactive way—only after an illegal surveillance were discovered would its validity be determined.[162] The second approach, while protecting both the national security and personal liberties to a limited extent, would still lend itself to executive abuse. The determination of what are exigent circumstances will necessarily be a subjective judgment on the part of the government. In the light of past abuses, the protection afforded by this approach seems inadequate.[163] The third approach, while appearing to protect personal liberties absolutely, would seriously jeopardize the national security. Placing the national security in this precarious position, in turn, jeopardizes the personal liberties thought to be protected since the liberties granted by our constitutional form of government are no more secure than the government itself. The President, faced with an emergency situation, could not act with the required speed and thus would be prevented from fulfilling his constitutional duty. Indeed, inasmuch as this approach would prevent the President from fulfilling his constitutional responsibility, it is, most likely, unconstitutional.[164]

These deficiencies noted, it seems the better course for Congress to provide comprehensive legislation along the lines of the Foreign Intelligence Act. Such legislation is capable of affording a greater degree of protection to both the national security and personal liberty. It could be tailored in such a way that the question of whether or not a given situation required prior judicial authorization would require little or no guesswork on the part of the Government. The Foreign Intelligence Security Act represents just such a comprehensive approach at filling the national security gap. Its provisions are sufficiently definite to protect the individual's liberties from governmental abuse yet flexible enough to provide for an emergency situation where the national security demands governmental action without prior judicial authorization. In essence, this Act appears to strike the necessary balance between the need for intelligence surveillance and the protection of personal liberties from its uncontrolled use. Hopefully, a similar act will be high on the list of Congressional priorities in 1977.

Charles G. La Bella

161. This approach seems to have been adopted by the Supreme Court in Keith. Since the argument of delay never came up, the Court did not consider what would happen in the case of an emergency situation where the President had to act quickly. One can only assume the Court would create an exception in such a situation where the domestic security was threatened. Cf. United States v. United States Dist. Court, 407 U.S. at 318.

162. See United States v. Butenko, 494 F.2d 593, 605 (3d Cir.) (en banc), cert. denied 419 U.S. 881 (1974). Cf. United States v. United States Dist. Court, 407 U.S. at 316-18.

163. See note 21 supra.

164. Cf. United States v. United States Dist. Court, 407 U.S. at 310.

APPENDIX D

C. EXCESSIVE USE OF INTRUSIVE TECHNIQUES

MAJOR FINDING

The intelligence community has employed surreptitious collection techniques—mail opening, surreptitious entries, informants, and "traditional" and highly sophisticated forms of electronic surveillance—to achieve its overly broad intelligence targeting and collection objectives. Although there are circumstances where these techniques, if properly controlled, are legal and appropriate, the Committee finds that their very nature makes them a threat to the personal privacy and Constitutionally protected activities of both the targets and of persons who communicate with or associate with the targets. The dangers inherent in the use of these techniques have been compounded by the lack of adequate standards limiting their use and by the absence of review by neutral authorities outside the intelligence agencies. As a consequence, these techniques have collected enormous amounts of personal and political information serving no legitimate governmental interest.

Subfindings

(a) Given the highly intrusive nature of these techniques,[1] the legal standards and procedures regulating their use have been insufficient. There have been no statutory controls on the use of informants; there have been gaps and exceptions in the law of electronic surveillance; and the legal prohibitions against warrantless mail opening and surreptitious entries have been ignored.

(b) In addition to providing the means by which the Government can collect too much information about too many people, certain techniques have their own peculiar dangers:

(i) Informants have provoked and participated in violence and other illegal activities in order to maintain their cover, and they have obtained membership lists and other private documents.

(ii) Scientific and technological advances have rendered traditional controls on electronic surveillance obsolete and have made it more difficult to limit intrusions. Because of the nature of wiretaps, microphones and other sophisticated electronic techniques, it has not always been possible to restrict the monitoring of communications to the persons being investigated.

(c) The imprecision and manipulation of labels such as "national

[1] The techniques noted here do not constitute an exhaustive list of the surreptitious means by which intelligence agencies have collected information. The FBI, for example, has obtained a great deal of financial information about American citizens from tax returns filed with the Internal Revenue Service. (See IRS Report: Sec. I, "IRS Disclosures to FBI and CIA.") This section, however, is limited to problems raised by electronic surveillance, mail opening, surreptitious entries informants and electronic surveillances.

security," "domestic security," "subversive activities," and "foreign intelligence" have led to unjustified use of these techniques.

Elaboration of Findings

The preceding section described how the absence of rigorous standards for opening, controlling, and terminating investigations subjected many diverse elements of this society to scrutiny by intelligence agencies, without their being suspected of violating any law. Once an investigation was opened, almost any item of information about a target's personal behavior or political views was considered worth collecting.

Extremely intrusive techniques—such as those listed above—have often been used to accomplish those overly broad targeting and collection objectives.

The paid and directed informant has been the most extensively used technique in FBI domestic intelligence investigations. Informants were used in 83% of the domestic intelligence investigations analyzed in a recent study by the General Accounting Office.[1a] As of June 30, 1975, the FBI was using a total of 1,500 domestic intelligence informants.[2] In 1972 there were over 7,000 informants in the ghetto informant program alone. In fiscal year 1976, the Bureau has budgeted more than $7.4 million for its domestic intelligence informant program, more than twice the amount allocated for its organized crime informant program.[3]

Wiretaps and microphones have also been a significant means of gathering intelligence. Until 1972, the FBI directed these electronic techniques against scores of American citizens and domestic organizations during investigations of such matters as domestic "subversive" activities and leaks of classified information. The Bureau continues to use these techniques against foreign targets in the United States.

The most extensive use of electronic surveillance has been by the National Security Agency. NSA has electronically monitored (without wiretapping in the traditional sense) international communication links since its inception in 1952; because of its sophisticated technology, it is capable of intercepting and recording an enormous number of communications between the United States and foreign countries.[4]

All mail opening programs have now been terminated, but a total of twelve such operations were conducted by the CIA and the FBI in ten American cities between 1940 and 1973.[5] Four of these were operated by the CIA, whose most massive project involved the opening of more than 215,000 letters between the United States and the Soviet Union over a twenty-year period. The FBI conducted eight mail opening programs, three of which included opening mail sent between two points in the United States. The longest FBI mail opening program

[1a] Report to the House Committee on the Judiciary, by the Comptroller General of the United States, "FBI Domestic Intelligence Operations—Their purpose and scope: Issues that Need to be Resolved," 2/24/76, p. 96.

[2] FBI memorandum to the Select Committee, 11/28/75.

[3] Memorandum, *FBI Overall Intelligence Program FY 1977 Compared to FY 1976* undated. The cost of the intelligence informant program comprises payments to informants for services and expense as well as the costs of FBI personnel, support and overhead.

[4] See NSA Report: Sec. I, "Introduction and Summary."

[5] See Mail Opening Reports: Sec. I, "Summary and Principal Conclusions."

lasted, with one period of suspension, for approximately twenty-six years.

The FBI has also conducted hundreds of warrantless surreptitious entries—break-ins—during the past twenty-five years. Often these entries were conducted to install electronic listening devices; at other times they involved physical searches for information. The widespread use of warrantless surreptitious entries against both foreign and domestic targets was terminated by the Bureau in 1966 but the FBI has occasionally made such entries against foreign targets in more recent years.

All of these techniques have been turned against American citizens as well as against certain foreign targets. On the theory that the executive's responsibility in the area of "national security" and "foreign intelligence" justified their use without the need of judicial supervision, the intelligence community believed it was free to direct these techniques against individuals and organizations whom it believed threatened the country's security. The standards governing the use of these techniques have been imprecise and susceptible to expansive interpretation and in the absence of any judicial check on the application of these vague standards to particular cases, it was relatively easy for intelligence agencies and their superiors to extend them to many cases where they were clearly inappropriate. Lax internal controls on the use of some of these techniques compounded the problem.

These intrusive techniques by their very nature invaded the private communications and activities both of the individuals they were directed against and of the persons with whom the targets communicated or associated. Consequently, they provided the means by which all types of information—including personal and political information totally unrelated to any legitimate governmental objective—were collected and in some cases disseminated to the highest levels of the government.

Subfinding (a)

Given the highly intrusive nature of these techniques, the legal standards and procedures regulating their use have been insufficient. There have been no statutory controls on the use of informants; there have been gaps and exceptions in the law of electronic surveillance; and the legal prohibitions against warrantless mail opening and surreptitious entries have been ignored.

1. The Absence of Statutory Restraints on the Use of Informants

There are no statutes or published regulations governing the use of informants.[6] Consequently, the FBI is free to use informants, guided only by its own internal directives which can be changed at any time by FBI officials without approval from outside the Bureau.[7]

[6] Title 28 of the United States Code provides only that appropriations for the Department of Justice are available for payment of informants. 28 U.S.C. § 524.

[7] The Attorney General has announced that he will issue guidelines on the use of informants in the near future, and our recommendations provide standards for informant control and prohibitions on informant activity. (See pp. 328.) In addition, the Attorney General's recently promulgated guidelines on "Domestic Security Investigations" limit the use of informants at the early stages of such inquiries and provide for review by the Justice Department of the initiation of "full investigations" in which new informants may be recruited.

Apart from court decisions precluding the use of informants to entrap persons into criminal activity, there are few judicial opinions dealing with informants and most of those concern criminal rather than intelligence informants.[8] The United States Supreme Court has never ruled on whether the use of intelligence informants in the contexts revealed by the Committee's investigation offend First Amendment rights of freedom of expression and association.[9]

In the absence of regulation through statute, published regulation, or court decision, the FBI has used informants to report on virtually every aspect of a targeted group or individual's activity, including lawful political expression, political meetings, the identities of group members and their associates, the "thoughts and feelings, intentions and ambitions," of members,[10] and personal matters irrelevant to any legitimate governmental interest. Informants have also been used by the FBI to obtain the confidential records and documents of a group.[11]

Informants could be used in any intelligence investigation. FBI directives have not limited informant reporting to actual or likely violence or other violations of law.[12] Nor has any determination been made concerning whether the substantial intrusion represented by informant coverage is justified by the government's interest in obtaining information, or whether less intrusive means would adequately serve the government's interest. There has also been no requirement that the decisions of FBI officials to use informants be reviewed by anyone outside the FBI. In short, intelligence informant coverage has not been subject to the standards which govern the use of other intrusive techniques such as electronic surveillance, even though informants can produce a far broader range of information.

2. Gaps and Exceptions in the Law of Electronic Surveillance

Congress and the Supreme Court have both addressed the legal issues raised by electronic surveillance, but the law has been riddled with gaps and exceptions. The Executive branch has been able to apply vague standards for the use of this technique to particular cases

---

[8] In a criminal case involving charges of jury bribery, *United States* v. *Hoffa*, 385 U.S. 293 (1966), the Supreme Court ruled that an informant's testimony concerning conversations of a defendant could not be considered the product of a warrantless search in violation of the Fourth Amendment on the ground the defendant had consented to the presence of the informant. In another criminal case, *Lewis* v. *United States*, 385 U.S. 206 (1966), the Court stated that "in the detection of many types of crimes, the Government is entitled to use decoys and to conceal the identity of its agents."

[9] In a more recent case, the California Supreme Court held that secret surveillance of classes and group meetings at a university through the use of undercover agents was "likely to pose a substantial restraint upon the exercise of First Amendment rights." *White* v. *Davis*, 533 Pac. Rep. 2d, 223 (1975) Citing a number of U.S. Supreme Court opinions, the California Supreme Court stated in its unanimous decision:

"In view of this significant potential chilling effect, the challenged surveillance activities can only be sustained if [the Government] can demonstrate a 'compelling' state interest which justifies the resultant deterrence of First Amendment rights and which cannot be served by alternative means less instrusive on fundamental rights." 533 Pac. Rep. 2d, at 232

[10] Gary Rowe testimony, 12/2/75 Hearings, Vol. 6, pp. 111, 118.

[11] Cook, 12/2/75, Hearings, Vol. 6, p. 111.

[12] The FBI Manual of Instructions proscribes only reporting of privileged communications between an attorney and client, legal "defense plans or strategy," "employer-employee relationships" (where an informant is connected with a labor union), and "legitimate institution or campus activities" at schools. (FBI Manual Section 107.)

as it has seen fit, and, in the case of NSA monitoring, the standards and procedures for the use of electronic surveillance were not applied at all.

When the Supreme Court first considered wiretapping, it held that the warrantless use of this technique was constitutional because the Fourth Amendment's warrant requirement applied only to physical trespass and did not extend to the seizure of conversation. This decision, the 1928 case of *Olmstead* v. *United States*, involved a criminal prosecution, and left federal agencies free to engage in the unrestricted use of wiretaps in both criminal and intelligence investigations.[13]

Six years later, Congress enacted the Federal Communications Act of 1934, which made it a crime for "any person," without authorization, to intercept and divulge or publish the contents of wire and radio communications. The Supreme Court subsequently construed this section to apply to federal agents as well as to ordinary citizens, and held that evidence obtained directly or indirectly from the interception of wire and radio communications was not admissible in court.[14] But Congress acquiesed in the Justice Department's position that these cases prohibited only the divulgence of contents of wire communications outside the executive branch,[15] and Government wiretapping for intelligence purposes other than prosecution continued.

On the ground that neither the 1934 Act nor the Supreme Court decisions on wiretapping were meant to apply to "grave matters involving the defense of the nation," President Franklin Roosevelt authorized Attorney General Jackson in 1940 to approve wiretaps on "persons suspected of subversive activities against the Government of the United States, including suspected spies."[16] In the absence of any guidance from Congress or the Court for another quarter century, the executive branch first broadened this standard in 1946 to permit wiretapping in "cases vitally affecting the domestic security or where human life is in jeopardy,"[17] and then modified it in 1965 to allow wiretapping in "investigations related to the national security."[18] Internal Justice Department policy required the prior approval of the Attorney General before the FBI could institute wiretaps in particular cases,[19] but until the mid-1960's there was no require-

[13] *Olmstead* v. *United States*, 277 U.S. 438 (1928).

[14] *Nardone* v. *United States*, 302 U.S. 397 (1937); 308 U.S. 338 (1939).

[15] For example, letter from Attorney General Jackson to Rep. Hatton Summers, 3/19/41; See Electronic Surveillance Report: Sec. II.

[16] Memorandum from President Roosevelt to the Attorney General 5/21/40.

[17] Letter from Attorney General Tom C. Clark to President Truman, 7/17/46.

[18] Directive from President Johnson to Heads of Agencies, 6/30/65.

[19] President Roosevelt's 1940 order directed the Attorney General to approve wiretaps "after investigation of the need in each case." (Memorandum from President Roosevelt to Attorney General Jackson, 5/21/40.) However, Attorney General Francis Biddle recalled that Attorney General Jackson "turned it over to Edgar Hoover without himself passing on each case" in 1940 and 1941. Biddle's practice beginning in 1941 conformed to the President's order. (Francis Biddle, *In Brief Authority* (Garden City: Doubleday, 1962), p. 167.)

Since 1965, explicit written authorization has been required. (Directive of President Johnson 6/30/65.) This requirement however, has often been disregarded. In violation of this requirement, for example, no written authorizations were obtained from the Attorney General—or from any one else—for a series of four wiretaps implemented in 1971 and 1972 on Yeoman Charles Radford, two of his friends, and his father-in-law. See Electronics Surveillance Report; Sec. VI.

(Continued)

ment of periodic reapproval by the Attorney General.[20] In the absence of any instruction to terminate them, some wiretaps remained in effect for years.[21]

In 1967, the Supreme Court reversed its holding in the *Olmstead* case and decided that the Fourth Amendment's warrant requirement did apply to electronic surveillances.[22] It expressly declined, however, to extend this holding to cases involving the "national security." [22a] Congress followed suit the next year in the Omnibus Crime Control Act of 1968, which established a warrant procedure for electronic surveillance in criminal cases but included a provision that neither it nor the Federal Communications Act of 1934 "shall limit the constitutional power of the President." [23] Although Congress did not purport to define the President's power, the Act referred to five broad categories which thereafter served as the Justice Department's criteria for warrantless electronic surveillance. The first three categories related to foreign intelligence and counterintelligence matters:

(1) to protect the Nation against actual or potential attack or other hostile acts of a foreign power;

(2) to obtain foreign intelligence information deemed essential to the security of the United States; and

(3) to protect the national security information against foreign intelligence activities.

The last two categories dealt with domestic intelligence interests:

(4) to protect the United States against overthrow of the government by force or other unlawful means, or

(5) against any other clear and present danger to the structure or existence of the government.

In 1972, the Supreme Court held in *United States* v. *United States District Court*,[22a] that the President did not have the constitutional power to authorize warrantless electronic surveillances to protect the

---

(Continued)
The first and third of these taps were implemented at the oral instruction of Attorney General John Mitchell. (Memorandum from T. J. Smith E. S. Miller, 2/26/73.) The remaining taps were implemented at the oral request of David Young, and assistant to John Ehrlichman at the White House, who merely informed the Bureau that the requests originated with Ehrlichman and had the Attorney General's concurrence. (Memorandum from T. J. Smith to E. S. Miller, 6/14/73.

[20] Attorney General Nicholas Katzenbach instituted this requirement in March 1965. (Memorandum from J. Edgar Hoover to the Attorney General, 3/3/65.)

[21] The FBI maintained one wiretap on an official of the Nation of Islam that had originally been authorized by Attorney General Brownell in 1957 for seven years until 1964 without any subsequent re-authorization. (Memorandum from J. Edgar Hoover to the Attorney General, 12/31/65, initialed "Approved: HB, 1/2/57.")

As Nicholas Katzenbach testified: "The custom was not to put a time limit on a tap, or any wiretap authorization. Indeed, I think the Bureau would have felt free in 1965 to put a tap on a phone authorized by Attorney General Jackson before World War II." (Nicholas Katzenbach testimony, 11/12/75, p. 87.)

[22] *Katz* v. *United States*, 389 U.S. 347 (1967).

[22a] The Court wrote: "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case." 389 U.S. at 358 n. 23.

[23] 18 U.S.C. 2511 (3).

[22a] 407 U.S. 297 (1972)

nation from domestic threats.[24] The Court pointedly refrained, however, from any "judgment on the scope of the Presidents' surveillance power with respect to the activities of foreign powers, within or without this country." [25] Only "the domestic aspects of national security" came within the ambit of the Court's decision.[26]

To conform with the holding in this case, the Justice Department thereafter limited warrantless wire tapping to cases involving a "significant connection with a foreign power, its agents or agencies.[27]

At no time, however, were the Justice Department's standards and procedures ever applied to NSA's electronic monitoring system and its "watch listing" of American citizens.[28] From the early 1960's until 1973, NSA compiled a list of individuals and organizations, including 1200 American citizens and domestic groups, whose communications were segregated from the mass of communications intercepted by the Agency, transcribed, and frequently disseminated to other agencies for intelligence purposes.[29]

The Americans on this list, many of whom were active in the anti-war and civil rights movements, were placed there by the FBI, CIA, Secret Service, Defense Department, and NSA itself without prior judicial warrant or even the prior approval of the Attorney General. In 1970, NSA began to monitor telephone communications links between the United States and South America at the request of the Bureau of Narcotics and Dangerous Drugs (BNDD) to obtain information about international drug trafficking. BNDD subsequently submitted the names of 450 American citizens for inclusion on the

---

[24] At the same time, the Court recognized that "domestic security surveillance" may involve different policy and practical considerations apart from the surveillance of 'ordinary crime,' 407 U.S. at 321, and thus did not hold that "the same type of standards and procedures prescribed by Title III [of the 1968 Act] are necessarily applicable to this case." (407 U.S. at 321.) The Court noted:

"Given the potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crime in Title III. Different standards may be compatible with the Fourt Amendment." (407 U.S. at 321.)

[25] 407 U.S. at 307.

[26] 407 U.S. at 320. *United States* v. *United States District Court* remains the only Supreme Court case dealing with the issue of warrantless electronic surveillance for intelligence purposes. Three federal circuit courts have considered this issue since 1972, however. The Third Circuit and the Fifth Circuit both held that the President may constitutionally authorize warrantless electronic surveillance for foreign counterespionage and foreign intelligence purposes. [*United States* v. *Butenko*, 494 F.2d 593 (3d Cir. 1974), *cert. denied sub nom. Ivanov* v. *United States*, 419 U.S. 881 (1974); and *United States* v. *Brown*, 484 F.2d 418 (5th Cir., 1973), *cert. denied* 415 U.S. 960 (1974).] The District of Columbia Circuit held unconstitutional the warrantless electronic surveillance of the Jewish Defense League, a domestic organization whose activities allegedly affected U.S. Soviet relations but which was neither the agent of nor in collaboration with a foreign power. [*Zweibon* v. *Mitchell*, 516 F.2d 594 (D.C. Cir., 1975) (*en banc*).]

[27] Testimony of Deputy Assistant Attorney General Kevin Maroney, Hearings before the Senate Subcommittee on Administrative Practice and Procedures, 6/29/72, p. 10. This language paralled that of the Court in *United States* v. *United States District Court*, 407 U.S. at 309 n. 8.

[28] Although Attorney General John Mitchell and Justice Department officials on the Intelligence Evalnation Committee apparently learned that NSA was making a contribution to domestic intelligence in 1971, there is no indication that the FBI told them of its submission of names of Americans for inclusion on a NSA "watch list." When Assistant Attorney General Henry Petersen learned of these practices in 1973, Attorney General Elliott Richardson ordered that they be terminated. (See Report on NSA: Sec. I, "Introduction and Summary.")

[29] See NSA Report: Sec. I, "Introduction and Summary."

Watch List, again without warrant or the approval of the Attorney General.[30]

The legal standards and procedures regulating the use of microphone surveillance have traditionally been even more lax than those regulating the use of wiretapping. The first major Supreme Court decision on microphone surveillance was *Goldman* v. *United States*, 316 U.S. 129 (1942), which held that such surveillance in a criminal case was constitutional when the installation did not involve a trespass. Citing this case, Attorney General McGrath prohibited the trespassory use of this technique by the FBI in 1952.[31] But two years later—a few weeks after the Supreme Court denounced the use of a microphone installation in a criminal defendant's bedroom [32]—Attorney General Brownell gave the FBI sweeping authority to engage in bugging for intelligence purposes. ". . . (C)onsiderations of internal security and the national safety are paramount," he wrote, "and, therefore, may compel the unrestricted use of this technique in the national interest." [33]

Since Brownell did not require the prior approval of the Attorney General for bugging specific targets, he largely undercut the policy that had developed for wiretapping. The FBI in many cases could obtain equivalent coverage by utilizing bugs rather than taps and would not be burdened with the necessity of a formal request to the Attorney General.

The vague "national interest" standards established by Brownell, and the policy of not requiring the Attorney General's prior approval for microphone installations, continued until 1965, when the Justice Department began to apply the same criteria and procedures to both microphone and telephone surveillance.

3. Ignoring the Prohibitions Against Warrantless Mail Opening and Surreptitious Entries

Warrantless mail opening and surreptious entries, unlike the use of informants and electronic surveillance, have been clearly prohibited by both statutory and constitutional law. In violation of these prohibitions, the FBI and the CIA decided on their own when and how these techniques should be used.[35]

Sections 1701 through 1973 of Title 18 of the United States Code forbid persons other than employees of the Postal Service "dead letter" office from tampering with or opening mail that is not addressed to them. Violations of these statutes may result in fines of up to $2000

[30] Memorandum from Iredell to Gayler, 4/10/70; See NSA Report: Sec. I, Introduction and Summary. BNDD originally requested NSA to monitor the South American link because it did not believe it had authority to wiretap a few public telephones in New York City from which drug deals were apparently being arranged. (Iredell testimony, 9/18/75, p. 99.)

[31] Memorandum from the Attorney General to Mr. Hoover, 2/26/52.

[32] *Irvine* v. *California*, 347 U.S. 128 (1954).

[33] Memorandum from the Attorney General to the Director, FBI, 5/20/54.

[35] While such techniques might have been authorized by Attorneys General under expansive "internal security" or "national interest" theories similar to Brownell's authorization for installing microphones by trespass, the issue was never presented to them for decision before 1967, when Attorney General Ramsey Clark turned down a surreptitious entry request. There is no indication that the legal questions were considered in any depth in 1970 or 1971 at the time of the "Huston Plan" and its aftermath. See Huston Plan Report: Sec. III, Who, What, When and Where.

and imprisonment for not more than five years. The Supreme Court has also held that both First Amendment and Fourth Amendment restrictions apply to mail opening.

The Fourth Amendment concerns were articulated as early as 1878, when the Court wrote:

> The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant . . . as is required when papers are subjected to search in one's own household.[36]

This principle was reaffirmed as recently as 1970 in *United States* v. *Van Leeuwen*, 396 U.S. 249 (1970). The infringement of citizens' First Amendment rights resulting from warrantless mail opening was first recognized by Justice Holmes in 1921. "The use of the mails," he wrote in a dissent now embraced by prevailing legal opinion, "is almost as much a part of free speech as the right to use our tongues."[37] This principle, too, has been affirmed in recent years.[38]

Breaking and entering is a common law felony as well as a violation of state and federal statutes. When committed by Government agents, it has long been recognized as "the chief evil against which the wording of the Fourth Amendment is directed."[39]

In the one judicial decision concerning the legality of warrantless "national security" break-ins for physical search purposes, United States District Court Judge Gerhard Gesell held such entries unconstitutional. This case, *United States* v. *Ehrlichman*,[40] involved an entry into the office of a Los Angeles psychiatrist, Dr. Lewis Fielding, to obtain the medical records of his client Daniel Ellsberg, who was then under federal indictment for revealing classified documents. The entry was approved by two Presidential assistants, John Ehrlichman and Charles Colson, who argued that it had been justified "in the national interest." Ruling on the defendants' discovery motions, Judge Gesell found that because no search warrant was obtained:

> The search of Dr. Fielding's office was clearly illegal under the unambiguous mandate of the Fourth Amendment. . . . [T]he Government must comply with the strict constitutional and statutory limitations on trespassory searches and arrests even when known foreign agents are involved. . . . To hold otherwise, except under the most exigent circumstances, would be to abandon the Fourth Amendment to the whim of the Executive in total disregard of the Amendment's history and purpose.[41]

[36] *Ex Parte Jackson*, 96, U.S. 727, 733 (1878).
[37] *Milwaukee Pub. Co.* v. *Burleson*, 255 U.S. 407, 437 (1921) (dissent).
[38] See *Lamont* v. *Postmaster General*, 381 U.S. 301 (1965); *Procunier* v. *Martinez*, 416 U.S. 396 (1975).
[39] *United States* v. *United States District Court*, 407 US 297, 313 (1972).
[40] 376 F. Supp. 29, (D.D.C. 1974).
[41] 376 F. Supp. at 33.

94-523 O - 78 - 13

In the appeal of this decision, the Justice Department has taken the position that a physical search may be authorized by the Attorney General without a warrant for "foreign intelligence" proposes.[42] The warrantless mail opening programs and surreptitious entries by the FBI and CIA did not even conform to the "foreign intelligence" standard, however, now were they specifically approved in each case by the Attorney General. Domestic "subversives" and "extremists" were targeted for mail opening; and domestic "subversives" and "White Hate groups" were among those targeted for surreptitious entries.[43] Until the Justice Department's recent statement in the Ehrlichman case, moreover, no legal justification had ever been advanced publicly for violating the statutory or constitutional prohibitions against physical searches or opening mail without a judicial warrant, and none has ever been officially advanced by any Administration to justify warrantless mail openings.

Subfinding (b)

In addition to providing the means by which the Government can collect too much information about too many people, certain techniques have their own peculiar dangers:

(i) Informants have provoked and participated in violence and other illegal activities in order to maintain their cover, and they have obtained membership lists and other private documents.

(ii) Scientific and technological advances have rendered obsolete traditional controls on electronic surveillance obsolete and have made it more difficult to limit intrusions. Because of the nature of wiretaps, microphones, and other sophisticated electronic techniques, it has not always been possible to restrict the monitoring of communications to the persons being investigated.

a. The Intrusive Nature of the Intelligence Informant Technique

The FBI employs two types of informants: (1) "intelligence informants" who are used to report on groups and individuals in the course of intelligence investigations, and (2) "criminal informants," who are used in connection with investigations of specific criminal activity. FBI intelligence informants are administered by the FBI Intelligence Division at Bureau headquarters through a centralized system that is separate from the administrative system for FBI criminal informants. For example, the FBI's large-scale Ghetto Informant Program was administered by the FBI Intelligence Division. The Committee's investigation centered on the use of FBI intelligence informants. The FBI's criminal informant program fell outside the scope of the Committee's mandate, and accordingly it was not examined.

The Committee recognizes that FBI intelligence informants in violent groups have sometimes played a key role in the enforcement of

[42] Letter from Acting Assistant Attorney General John C. Keeny to Hugh E. Kline, Clerk of the U.S. Court of Appeals for the District of Columbia, 5/9/75.

[43] The Supreme Court's decision in *United States* v. *United States District Court*, 407 U.S. 297 (1972), clearly established the principle that such warrantless invasions of the privacy of Americans are unconstitutional.

the criminal law. The Committee examined a number of such cases,[44] and in public hearings on the use of FBI intelligence informants included the testimony of a former informant in the Ku Klux Klan whose reporting and court room testimony was essential to the arrest and conviction of the murderers of Mrs. Viola Liuzzo, a civil rights worker killed in 1965.[45] Former Attorney General Katzenbach testified that informants were vital to the solution of the murders of three civil rights workers killed in Mississippi in 1964.[46]

FBI informant coverage of the Women's Liberation Movement resulted in intensive reporting on the identities and opinions of women who attended WLM meetings. For example, the FBI's New York Field Office summarized one informant's report in a memorandum to FBI Headquarters:

> Informant advised that a WLM meeting was held on _____.[47] Each woman at this meeting stated why she had come to the meeting and how she felt oppressed, sexually or otherwise.
>
> According to this informant, these women are mostly concerned with liberating women from this "oppressive society." They are mostly against marriage, children, and other states of oppression caused by men. Few of them, according to the informant, have had political backgrounds.[48]

Individual women who attended WLM meetings at midwestern universities were identified by FBI intelligence informants. A report by the Kansas City FBI Field Office stated:

> Informant indicates members of Women's Liberation campus group who are now enrolled as students at University of Missouri, Kansas City, are _____, _____; _____, _____, _____.[49] Informant noted that _____, and _____,[50] not currently students on the UMKC campus are reportedly roommates at _____.[51]

---

[44] In one case, an FBI informant involved in an intelligence investigation of the Detroit Black Panther Party furnished advance information regarding a planned ambush of Detroit police officers which enabled the Detroit Police Department to take necessary action to prevent injury or death to the officers and resulted in the arrest of eight persons and the seizure of a cache of weapons. The informant also furnished information resulting in the location and confiscation by Bureau agents of approximately fifty sticks of dynamite available to the Black Panther Party which likely resulted in the saving of lives and the prevention of property damage. (Joseph Deegan testimony, 2/13/76, p. 54)

[45] Rowe, 12/2/75, Hearings, Vol. 6, p. 115.

[46] Katzenbach testified that the case "could not have been solved without acquiring informants who were highly placed members of the Klan." (Katzenbach, 12/3/75, Hearings, Vol. 6, p. 215.)

[47] Date and address deleted at FBI request so as not to reveal informant's identity.

[48] Memorandum, from New York Field Office to FBI Headquarters, re: Women's Liberation Movement, 5/28/69, p. 2.

[49] Names deleted for security reasons.

[50] Names deleted for security reasons.

[51] Names and addresses deleted for security reasons.

Informants were instructed to report "everything" they knew about a group to the FBI.

> . . . to go to meetings, write up reports . . . on what happened, who was there . . . to try to totally identify the background of every person there, what their relationships were, who they were living with, who they were sleeping with, to try to get some sense of the local structure and the local relationships among the people in the organization.[52]

Another intelligence informant described his mission as "total reporting." Rowe testified that he reported "anything and everything I observed or heard" pertaining to any member of the group he infiltrated.[53]

Even where intelligence informants are used to infiltrate groups where some members are suspected of violent activity, the nature of the intelligence mission results in governmental intrusion into matters irrelevant to that inquiry. The FBI Special Agents who directed an intelligence informant in the Ku Klux Klan testified that the informant

> . . . furnished us information on the meetings and the thoughts and feelings, intentions and ambitions, as best he knew them, of other members of the Klan, both the rank and file and the leadership.[54]

Intelligence informants also report on other groups—not the subject of intelligence investigations—which merely associate with, or are even opposed to, the targeted group. For example, an FBI informant in the VVAW had the following exchange with a member of the Committee:

> Senator HART (Mich.). . . . did you report also on groups and individuals outside the [VVAW], such as other peace groups or individuals who were opposed to the war whom you came in contact with because they were cooperating with the [VVAW] in connection with protest demonstrations and petitions?
>
> Ms. COOK. . . . I ended up reporting on groups like the United Church of Christ, American Civil Liberties Union, the National Lawyers Guild, liberal church organizations [which] quite often went into coalition with the VVAW.[55]

This informant reported the identities of an estimated 1,000 individuals to the FBI, although the local chapter to which she was assigned had only 55 regular members.[56] Similarly, an FBI informant in the Ku Klux Klan reported on the activities of civil rights and black groups that he observed in the course of his work in the Klan.[57]

In short, the intelligence informant technique is not a precise instrument. By its nature, it extends far beyond the sphere of proper govern-

[52] Cook, 12/2/75, Hearings, Vol. 6, p. 111.
[53] Rowe, 12/2/75, Hearings, Vol. 6, p. 116.
[54] Special Agent, 11/21/75, p. 7.
[55] Cook, 12/2/75, Hearings, Vol. 6, pp. 119, 120.
[56] Cook, 12/2/75, Hearings, Vol. 6, p. 120.
[57] Rowe, 12/2/75, Hearings, Vol. 6, p. 116.

mental interest and risks governmental monitoring of the private lives and the constitutionally-protected activity of Americans. Nor is the intelligence informant technique used infrequently. As reflected in the statistics described above, FBI intelligence investigations are in large part conducted through the use of informants; and FBI agents are instructed to "develop reliable informants at all levels and in all segments" of groups under investigation.[58]

b. Other Dangers in the Intelligence Informant Technique

In the absence of clear guidelines for informant conduct, FBI paid and directed intelligence informants have participated in violence and other illegal activities and have taken membership lists and other private documents.

1. Participation in Violence and Other Illegal Activity

The Committee's investigation has revealed that there is often a fundamental dilemma in the use of intelligence informants in violent organizations. The Committee recognizes that intelligence informants in such groups have sometimes played essential roles in the enforcement of the criminal law. At the same time, however, the Committee has found that the intelligence informant technique carries with it the substantial danger that informants will participate in, or provoke, violence or illegal activity. Intelligence informants are frequently infiltrated into groups for long-term reporting rather than to collect evidence for use in prosecutions. Consequently, intelligence informants must participate in the activity of the group they penetrate to preserve their cover for extended periods. Where the group is involved in violence or illegal activity, there is a substantial risk that the informant must also become involved in this activity. As an FBI Special Agent who handled an intelligence informant in the Ku Klux Klan testified: "[you] couldn't be an angel and be a good informant."[59]

FBI officials testified that it is Bureau practice to instruct informants that they are not to engage in violence or unlawful activity and, if they do so, they may be prosecuted. FBI Deputy Associate Director Adams testified:

> . . . we have informants who have gotten involved in the violation of the law, and we have immediately converted their status from an informant to the subject, and have prosecuted, I would say, offhand . . . around 20 informants.[60]

The Committee finds, however, that the existing guidelines dealing with informant conduct do not adequately ensure that intelligence informants stay within the law in carrying out their assignments. The FBI Manual of Instructions contain no provisions governing informant conduct. While FBI employee conduct regulations prohibit an FBI agent from directing informants to engage in violent or other illegal activity, informants themselves are not governed by these regulations since the FBI does not consider them as FBI employees.

[58] FBI Manual, Section 107 c(3).
[59] Special Agent, 11/21/75, p. 12.
[60] Adams, 12/2/75, Hearings, Vol. 6, p. 150.

In the absence of clear and precise written provisions directly applicable to informants, FBI intelligence informants have engaged in violent and other illegal activity. For example, an FBI intelligence informant who penetrated the Ku Klux Klan and reported on its activities for over five years testified that on a number of occassions he and other Klansmen had "beaten people severely, had boarded buses and kicked people off; had went in restaurants and beaten them with blackjacks, chains, pistols." [61] This informant described how he had taken part in Klan attacks on Freedom Riders at the Birmingham, Alabama, bus depot, where "baseball bats, clubs, chains and pistols" were used in beatings.[62]

Although the FBI Special Agents who directed this informant instructed him that he was not to engage in violence, it was recognized that there was a substantial risk that he would become a participant in violent activity.

As one of the Agents testified:

> ... it is kind of difficult to tell him that we would like you to be there on deck, observing, be able to give us information and still keep yourself detached and uninvolved and clean, and that was the problem that we constantly had.[63]

In another example, an FBI intelligence informant penetrated "right wing" groups operating in California under the names "The Minutemen" and "The Secret Army Oroganization." The informant reported on the activities of these "right wing" paramilitary groups for a period of five years but was also involved in acts of violence or destruction. In addition, the informant actually rose to a position of leadership in the SAO and became an innovator of various harassment actions. For example, he admittedly participated in firebombing of an automobile and was present, conducting a "surveillance" of a professor at San Diego State University, when his associate and subordinate in the SAO took out a gun and fired into the home of the professor, wounding a young woman.[64]

An FBI intelligence informant in a group of antiwar protesters planning to break into a draft board claimed to have provided technical instruction and materials that were essential to the illegal break- testified to the committee:

> Everything they learned about breaking into a building or climbing a wall or cutting glass or destroying lockers, I taught them. I got sample equipment, the type of windows that we would go through, I picked up off the job and taught them how to cut the glass, how to drill holes in the glass so you cannot hear it and stuff like that, and the FBI supplied me with the equipment needed. The stuff I did not have, the [the FBI] got off their own agents.[65]

The Committee finds that where informants are paid and directed by a government agency, the government has a responsibility to

[61] Rowe deposition, 10/17/75, p. 12.
[62] Rowe, 12/2/75, Hearings, Vol. 6, p. 118.
[63] Special Agent, 11/21/75, pp. 16–17.
[64] Memorandum from the FBI to Senate Select Committee, 2/26/76, with enclosures.
[65] Hardy, 9/29/75, pp. 16–17.

impose clear restrictions on their conduct. Unwritten practice or general provisions aimed at persons other than the informants themselves are not sufficient. In the investigation of violence or illegal activity, it is essential that the government not be implicated in such activity.

2. Membership Lists and Other Private Documents Obtained by the Government Through Intelligence Informants

The Committee finds that there are inadequate guidelines to regulate the conduct of intelligence informants with respect to private and confidential documents, such as membership lists, mailing lists and papers relating to legal matters. The Fourth Amendment provides that citizens shall be "secure in their . . . papers and effects, against unreasonable searches and seizures" and requires probable cause to believe there has been a violation of law before a search warrant may issue. Moreover the Supreme Court, in *NAACP* v. *Alabama*,[66] held that the First Amendment's protections of speech, assembly and group association did not permit a state to compel the production of the membership list of a group engaged in lawful activity. The Court distinguished the case where a state was able to demonstrate a "controlling justification" for such lists by showing a group's activities involved "acts of unlawful intimidation and violence." [66a]

There are no provisions in the FBI Manual which preclude the FBI from obtaining private and confidential documents through intelligence informants. The Manual does prohibit informant reporting of "any information pertaining to defense plans or strategy," but the FBI interprets this as applying only to privileged communications between an attorney and client in connection with a specific court proceeding.[67]

The Committee's investigation has shown that, the FBI, through its intelligence informants and sources, has sought to obtain membership lists and other confidential documents of groups and individuals.[68] For example, one FBI Special Agent testified:

> I remember one evening . . . [an informant] called my home and said I will meet you in a half an hour . . . I have a complete list of everybody that I have just taken out of the files, but I have to have it back within such a length of time.
>
> Well, naturally I left home and met him and had the list duplicated forthwith, and back in his possession and back in the files with nobody suspecting." [69]

Similarly, the FBI Special Agent who handled an intelligence informant in an antiwar group testified that he obtained confidential papers of the group which related to legal defense matters:

> "She brought back several things . . . various position papers taken by various legal defense groups, general statements of . . . the VVAW, legal thoughts on various trials, the

[66] 357 U.S. 449 (1958). Similarly, in *Bates* v. *City of Little Rock*, 361 U.S. 516 (1960), the Supreme Court held compulsory disclosure of group membership lists was an unjustified interference with members' freedom of association.
[66a] 361 U.S. at 465.
[67] FBI Manual of Instructions, Section 107.
[68] Surreptitious entry has also provided a means for the obtaining of such lists and other confidential documents.
[69] Special Agent, 11/19/75, pp. 10–11.

Gainesville (Florida) 8 . . . the Camden (New Jersey) 9 . . . various documents from all of these groups." [70]

This informant also testified that she took the confidential mailing list of the group she had penetrated and gave it to the FBI.[71]

She also gave the FBI a legal manual prepared by the group's attorneys to guide lawyers in defending the group's members should they be arrested in connection with antiwar demonstrations or other political activity.[72] Since this document was prepared as a general legal reference manual rather than in connection with a specific trial the FBI considered it outside the attorney-client privilege and not barred by the FBI Manual provision with respect to legal defense and strategy matters.

For the government to obtain membership lists and other private documents pertaining to lawful and protected activities covertly through intelligence informants risks infringing rights guaranteed by the Constitution. The Committee finds that there is a need for new guidelines for informant conduct with respect to the private papers of groups and individuals.

c. Electronic Surveillance

In the absence of judicial warrant, both the "traditional" forms of electronic surveillance practiced by the FBI—wiretapping and bugging—and the highly sophisticated form of electronic monitoring practiced by NSA have been used to collect too much information about too many people.

1. Wiretapping and Bugging

Wiretaps and bugs are considered by FBI officials to be one of the most valuable techniques for the collection of information relevant to the Bureau's legitimate foreign counterintelligence mandate. W. Raymond Wannall, the former Assistant Director in charge of the FBI's Intelligence Division, stated that electronic surveillance assisted Bureau officials in making "decisions" as to operations against foreigners engaged in espionage. "It gives us leads as to persons . . . hostile intelligence services are trying to subvert or utilize in the United States, so certainly it is a valuable technique." [73]

Despite its stated value in foreign counterintelligence cases, however, the dangers inherent in its use imply a clear need for rigorous controls. By their nature, wiretaps and bugs are incapable of a surgical precision that would permit intelligence agencies to overhear only the target's conversations. Since wiretaps are placed on particular telephones, anyone who uses a tapped phone—including members of the target's family—can be overheard. So, too, can everyone with whom the target (or anyone else using the target's telephone) communicates.[74] Microphones planted in the target's room or office inevitably intercept all conversations in a particular area: anyone conferring in the room or office, not just the target, is overheard.

[70] Special Agent, 11/20/75, pp. 15–16.
[71] Cook, 12/2/75, Hearings, Vol. 6, p. 112.
[72] Cook deposition, 10/14/75, p. 36.
[73] W. Raymond Wannall testimony, 10/21/75, p. 21.
[74] Under the Justice Department's procedures for Title III (court-ordered) wiretaps, however, the monitoring agent is obligated to turn off the recording equipment when certain privileged communications begin. Manual for conduct of Electronic Surveillance under Title III of Public Law 90–351, Sec. 8.1.

The intrusiveness of these techniques has a second aspect as well. It is extremely difficult, if not impossible, to limit the interception to conversations that are relevant to the purposes for which the surveillance is placed. Virtually all conversations are overheard, no matter how trivial, personal, or political they might be. When the electronic surveillance target is a political figure who is likely to discuss political affairs, or a lawyer, who confers with his clients, the possibilities for abuse are obviously heightened.

The dangers of indiscriminate interception are perhaps most acute in the case of microphones planted in locations such as bedrooms. When Attorney General Herbert Brownell gave the FBI sweeping authority to engage in microphone surveillances for intelligence purposes in 1954, he expressly permitted the Bureau to plant microphones in such locations if, in the sole discretion of the FBI, the facts warranted the installation.[75] Acting under this general authority, for example, the Bureau installed no fewer than twelve bugs in hotel rooms occupied by Dr. Martin Luther King, Jr.[76]

The King surveillances which occurred between January 1964 and October 1965, were ostensibly approved within the FBI for internal security reasons, but they produced vast amounts of personal information that were totally unrelated to any legitimate governmental interest; indeed, a single hotel room bug alone yielded twenty reels of tape that subsequently provided the basis for the dissemination of personal information about Dr. King throughout the Federal establishment.[76a] Significantly, FBI internal memoranda with respect to some of the installations make clear that they were planted in Dr. King's hotel rooms for the express purpose of obtaining personal information about him.[77]

Extremely personal information about the target, his family, and his friends, is easily obtained from wiretaps as well as microphones. This fact is clearly illustrated by the warrantless electronic surveillance of an American citizen who was suspected of leaking classified data to the press. A wiretap on this individual produced no evidence that he had in fact leaked any stories or documents, but among the items of information that the FBI did obtain from the tap (and delivered in utmost secrecy to the White House) were the following: that "meat was ordered [by the target's family] from a grocer;" that the target's daughter had a toothache; that the target needed grass clippings for a compost heap he was building; and that during a telephone conversation between the target's wife and a friend the "matters discussed were milk bills, hair, soap operas, and church." [78]

---

[75] Memorandum from the Attorney General to the Director, FBI, 5/20/54.

[76] Three additional bugs were planted in Dr. King's hotel rooms in 1965 after the standards for wiretapping and microphone surveillance became identical. According to FBI memoranda, apparently initiated by Katzenbach, Attorney General Nicholas Katzenbach was given after the fact notification that these three surveillances of Dr. King had occurred. See p. 273, and the King Report, Sec. IV, for further details.

[76a] Memorandum from F. J. Baumgardener to W. C. Sullivan, 3/26/64.

[77] For example, memorandum from Baumgardner to W. C. Sullivan, 2/4/64.

[78] FBI memoranda. Identifying details are being withheld by the Select Committee because of privacy considerations. Even the FBI realized that this type of information was unrelated to criminal activity or national security: for the last four months of this surveillance, most of the summaries that were disseminated to the White House began, "The following is a summary of nonpertinent information concerning captioned individual as of . . ."

The so-called "seventeen" wiretaps on journalists and government employees, which collectively lasted from May 1969 to February 1971, also illustrate the intrusiveness of electronic surveillance. According to former President Nixon, these taps produced "just gobs of material: gossip and bull." [79] FBI summaries of information obtained from the wiretaps and disseminated to the White House, suggest that the former President's private evaluation of them was correct. This wiretapping program did not reveal the source of any leaks of classified data, which was its ostensible purpose, but it did generate a wealth of information about the personal lives of the targets—their social contacts, their vacation plans, their employment satisfactions and dissatisfaction, their marital problems, their drinking habits, and even their sex lives.[80]

Among those who were incidentally overheard on one of these wiretaps was a currently sitting Associate Justice of the Supreme Court of the United States, who made plans to review a manuscript written by one of the targets.[81] Vast amounts of political information were also obtained from these wiretaps.[82]

The "seventeen" wiretaps also exemplify the particularly acute problems of wiretapping when the targeted individuals are involved in the domestic political process. These wiretaps produced vast amounts of purely political information,[82] much of which was obtained from the home telephones of two consultants to Senator Edmund Muskie and other Democratic politicians.

The incidental collection of political information from electronic surveillance is also shown by a series of telephone and microphone surveillances conducted during the Kennedy administration. In an investigation of the possibly unlawful attempts of representatives of a foreign country to influence congressional deliberations about sugar quota legislation in the early 1960s, Attorney General Robert Kennedy authorized a total of twelve warrantless wiretaps on foreign and domestic targets. Among the wiretaps of American citizens were two on American lobbyists, three on executive branch officials, and two on a staff member of a House of Representatives' Committee.[83] A bug was also planted in the hotel room of a United States Congressman, the Chairman of the House Agriculture Committee, Harold D. Cooley.[84]

Although this investigation was apparently initiated because of the Government's concern about future relations with the foreign country involved and the possibility of bribery,[85] it is clear that the Ken-

[79] Transcript of Presidential Tapes, 2/28/73 (House Judiciary Committee Statement of Information, Book VII, Part 4, p. 1754).

[80] For example, letters from Hoover to the Attorney General, 7/25/69, and 7/31/69; letters from Hoover to H. R. Haldeman, 6/25/70.

[81] Letter from Hoover to Haldeman, 6/25/70.

[82] Examples of such information are listed in the finding on Political Abuse, "The '17' wiretaps."

[83] Memorandum from J. Edgar Hoover to the Attorney General, 2/14/61; Memorandum from J. Edgar Hoover to the Attorney General, 2/16/61; Memorandum from J. Edgar Hoover to the Attorney General, 6/26/62; Memorandum from Wannall to W. C. Sullivan, 12/22/66.

[84] Memorandum from D. E. Moore to A. H. Belmont, 2/16/61.

[85] Memorandum from W. R. Wannall to W. C. Sullivan, 12/22/66; Memorandum from A. H. Belmont to Mr. Parsons, 2/14/61. This investigation did discover that representatives of a foreign nation were attempting to influence Congressional deliberations, but it did not reveal that money was being passed to any member of Congress or Congressional staff aide.

nedy administration was politically interested in the outcome of the sugar quota legislation as well.[86] Given the nature of the techniques used and of the targets they were directed against, it is not surprising that a great deal of potentially useful political information was generated from these "Sugar Lobby" surveillances.[87]

The highly intrusive nature of electronic surveillance also raises special problems when the targets are lawyers and journalists. Over the past two decades there have been a number of wiretaps placed on the office telephones of lawyers.[88] In the Sugar Lobby investigation, for example, Robert Kennedy authorized wiretaps on ten telephone lines of a single law firm.[90] All of these lines were apparently used by the one lawyer who was a target and presumably by other attorneys in the firm as well. Such wiretaps represent a serious threat to the attorney-client privilege, because once they are instituted they are capable of detecting all conversations between a lawyer and his clients, even those relating to pending criminal cases.

Since 1960, at least six American journalists and newsmen have also been the targets of warrantless wiretaps or bugs.[91] These surveillances were all rationalized as necessary to discover the source of leaks of classified information, but, since wiretaps and bugs are indiscriminate in the types of information collected, some of these taps revealed the attitudes of various newsmen toward certain politicians and supplied advance notice of forthcoming newspaper and magazine articles dealing with administration policies. The collection of information such as this, and the precedent set by wiretapping of newsmen, generally, inevitably tends to undermine the constitutional guarantee of a free and independent press.

2. NSA Monitoring

The National Security Agency (NSA) has the capability to monitor almost any electronic communication which travels through the air. This means that NSA is capable of intercepting a telephone call or even a telegram, if such call or telegram is transmitted at least partially through the air. Radio transmissions, *a fortiori*, are also within NSA's reach.

Since most communications today—to an increasing extent even domestic communications—are, at some point, transmitted through the air, NSA's potential to violate the privacy of American citizens is unmatched by any other intelligence agency. Furthermore, since the interception of electronic signals entails neither the installation of electronic surveillance devices nor the cooperation of private communications companies, the possibility that such interceptions will be undetected is enhanced.

NSA has never turned its monitoring apparatus upon entirely domestic communications, but from the early 1960s until 1973, it did inter-

[86] Memorandum from Wannall to W. C. Sullivan, 12/22/66.
[87] See Finding on Political Abuse, p. 233.
[88] Electronic Surveillance Report: Sec. II, "Presidential and Attorney General Authorization."
[90] Memorandum from J. Edgar Hoover to the Attorney General, 6/26/62.
[91] Memorandum from J. Edgar Hoover to the Attorney General 6/29/61; memorandum from J. Edgar Hoover to the Attorney General 7/31/62; memorandum from J. Edgar Hoover to the Attorney General 4/19/65; memorandum from J. Edgar Hoover to the Attorney General 6/4/69; memorandum from J. Edgar Hoover to the Attorney General 9/10/69; letter from W. C. Sullivan to J. Edgar Hoover 7/2/69.

cept the international communications of American citizens, without a warrant, at the request of other federal agencies.

Under current practice, NSA does not target any American citizen or firm for the purpose of intercepting their foreign communications. As a result of monitoring international links of communication, however, it does acquire an enormous number of communications to, from, or about American citizens and firms.[93]

As a practical matter, most of the communications of American citizens or firms acquired by NSA as incidental to its foreign intelligence-gathering process are destroyed upon recognition as a communication to or from an American citizen. But other such communications, which bear upon NSA's foreign intelligence requirements, are processed, and information obtained from them are used in NSA's reports to other intelligence agencies. Current practice precludes NSA from identifying American citizens and firms by name in such reports. Nonetheless, the practice does result in NSA's disseminating information derived from the international communications of American citizens and firms to the intelligence agencies and policymakers in the federal government.

In his dissent in *Olmstead* v. *United States*,[94] which held that the Fourth Amendment warrant requirement did not apply to the seizure of conversations by means of wiretapping, Justice Louis D. Brandeis expressed grave concern that new technologies might outstrip the ability of the Constitution to protect American citizens. He wrote:

> Subtler and more far-reaching means of invading privacy have become available to the government . . . (and) the progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home . . . . Can it be that the Constitution affords no protection against such invasions of individual security?

The question posed by Justice Brandeis applies with obvious force to the technological developments that allow NSA to monitor an enormous number of communications each year. His fears were firmly based, for in fact no warrant was ever obtained for the inclusion of 1200 American citizens on NSA's "Watch List" between the early 1960s and 1973, and none is obtained today for the dissemination within the intelligence community of information derived from the international communications of American citizens and firms. In the face of this new technology, it is well to remember the answer Justice Brandeis gave to his own question. Quoting from *Boyd* v. *United States*, 116 U.S. 616, he wrote:

> It is not the breaking of his doors, and the rummaging of his drawers that constitutes the essense of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property . . .[94a]

[93] NSA has long asserted that it had the authority to do this so long as one of the parties to such communication was located in a foreign country.

[94] 277 U.S. 438, 473–474 (1928).

[94a] 277 U.S. at 474–475.

D. Mail Opening

By ignoring the legal prohibitions against warrantless mail opening, the CIA and the FBI were able to obtain access to the written communications of hundreds of thousands of individuals, a large proportion of whom were American citizens. The intercepted letters were presumably sealed with the expectation that they would only be opened by the party to whom they were addressed, but intelligence agents in ten cities throughout the United States surreptitiously opened the seal and photographed the entire contents for inclusion in their intelligence files.

Mail opening is an imprecise technique. In addition to relying on a "Watch List" of names, the CIA opened vast numbers of letters on an entirely random basis; as one agent who opened mail in the CIA's New York project testified, "You never knew what you would hit." [95] Given the imprecision of the technique and the large quantity of correspondence that was opened, it is perhaps not surprising that during the twenty year course of the Agency's New York project, the mail that was randomly opened included that of at least three United States Senators and a Congressman, one Presidential Candidate, and numerous educational, business, and civil rights leaders.[96]

Several of the FBI programs utilized as selection criteria certain "indicators" on the outside of envelopes that suggested that the communication might be to or from a foreign espionage agent. These "indicators" were more refined than the "shotgun approach" [97] which characterized the CIA's New York project, and they did lead to the identification of three foreign spies.[98] But even by the Bureau's own accounting, it is clear that the mail of hundreds of innocent American citizens was opened and read for every successful counterintelligence lead that was obtained by means of "indicators." [99]

Large volumes of mail were also intercepted and opened in other FBI mail programs that were based not on indicators but on far less precise criteria. Two programs that involved the opening of mail to and from an Asian country, for example, used "letters to or from a university, scientific, or technical facility" as one selection criterion.[100] According to FBI memoranda, an average of 50 to 100 letters per day was opened and photographed during the ten years in which one of these two programs operated.[101]

[95] "CIA Officer" testimony, 9/30/75, p. 15.

[96] Staff summary of "Master Index," review, 9/5/75.

[97] James Angelton testimony, 9/17/75, p. 28.

[98] Wannall, 10/21/75, p. 5.

[99] In one of the programs based on "indicators" a participating agent testified that he opened 30 to 60 letters each day. (FBI agent statement, 9/10/75, p. 23.) In a second such program, a total of 1,011 letters were opened in one of the six cities in which it operated; statistics on the number of letters opened in the other five cities cannot be reconstructed. (W. Raymond Wannall testimony, 10/21/75, p. 5.) In a third such project, 2,350 letters were opened in one city and statistics for the other two cities in which it operated are unavailable. (Memorandum from W. A. Branigan to W. C. Sullivan, 8/31/61; Memorandum from Mr. Branigan to Mr. Sullivan, 12/21/61; memorandum from New York Field Office to FBI Headquarters, 3/5/62.)

[100] Letter from the FBI to the Senate Select Committee, 10/29/75. Six other criteria were used in these programs. See Mail Opening Report, Sec. IV.

[101] Memorandum from S. B. Donohoe to A. H. Belmont, 2/23/61; Memorandum from San Francisco Field Office to FBI Headquarters, 3/11/60. Statistics relating to the number of letters opened in the other program which used this criterion cannot be reconstructed.

E. Surreptitious Entries

Surreptitious entries, conducted in violation of the law, have also permitted intelligence agencies to gather a wide range of information about American citizens and domestic organization as well as foreign targets.[102] By definition this technique involves a physical entry into the private premises of individuals and groups. Once intelligence agents are inside, no "papers or effects" are secure. As the Huston Plan recommendations stated in 1970, "It amounts to burglary."[103]

The most private documents are rendered vulnerable by the use of surreptitious entries. According to a 1966 internal FBI memorandum, which discusses the use of this technique against domestic organizations:

> [The FBI has] on numerous occasions been able to obtain material held highly secret and closely guarded by subversive groups and organizations which consisted of membership lists and mailing lists of these organizations.[104]

A specific example cited in this memorandum also reveals the types of information that this technique can collect and the uses to which the information thus collected may be put:

> Through a "black bag" job, we obtained the records in the possession of three high-ranking officials of a Klan organization. . . . These records gave us the complete membership and financial information concerning the Klan's operation which we have been using most effectively to disrupt the organization and, in fact, to bring about its near disintegration.[105]

Unlike techniques such as electronic surveillance, government entries into private premises were familiar to the Founding Fathers. "Indeed," Judge Gesell wrote in the *Ehrlichman* case, "the American Revolution was sparked in part by the complaints of the colonists against the issuance of writs of assistance, pursuant to which the King's revenue officers conducted unrestricted, indiscriminate searches of persons and homes to uncover contraband."[106] Recognition of the intrusiveness of government break-ins was one of the primary reasons

---

[102] According to the FBI, "there were at least 239 surreptitious entries (for purposes other than microphone installation) conducted against at least fifteen domestic subversive targets from 1942 to April 1968. . . . In addition, at least three domestic subversive targets were the subject of numerous entries from October 1952 to June 1966." (FBI memorandum to the Senate Select Committee, 10/13/76.) One target, the Socialist Workers Party, was the subject of possibly as many as 92 break-ins by the FBI, between 1960 and 1966 alone. The home of at least one SWP member was also apparently broken into. (Sixth Supplementary Response to Requests for Production of Documents of Defendant, Director of the FBI, *Socialist Workers Party* v. *Attorney General*, 73 Civ. 3160, (SDNY), 3/24/76.) An entry against one "white hate group" was also reported by the FBI. (Memorandum from FBI Headquarters to the Senate Select Committee. 10/13/75.)

[103] Memorandum from Tom Huston to H. R. Haldeman, 7/70, p. 3.

[104] Memorandum from W. C. Sullivan to C. D. DeLoach, 7/19/66.

[105] Ibid.

[106] *United States* v. *Ehrlichman*, 376 F. Supp. 29, 32 (D.D.C. 1974).

for the subsequent adoption of the Fourth Amendment in 1791,[107] and this technique is certainly no less intrusive today.

Subfunding (c)

The imprecision and manipulation of labels such as "national security," "domestic security," "subversive activities" and "foreign intelligence" have led to unjustified use of these techniques.

Using labels such as "national security" and "foreign intelligence", intelligence agencies have directed these highly intrusive techniques against individuals and organizations who were suspected of no criminal activity and who posed no genuine threat to the national security. In the absence of precise standards and effective outside control, the selection of American citizens as targets has at times been predicated on grounds no more substantial than their lawful protests or their non-conformist philosophies. Almost any connection with any perceived danger to the country has sufficed.

The application of the "national security" rationale to cases lacking a substantial national security basis has been most apparent in the area of warrantless electronic surveillance. Indeed, the unjustified use of wiretaps and bugs under this and related labels has a long history. Among the wiretaps approved by Attorney General Francis Biddle under the standard of "persons suspected of subversive activities," for example, was one on the Los Angeles Chamber of Commerce in 1941.[108] This was approved in spite of his comment to J. Edgar Hoover that the target organization had "no record of espionage at this time." [109] In 1945, Attorney General Tom Clark authorized a wiretap on a former aide to President Roosevelt.[110] According to a memorandum by J. Edgar Hoover, Clark stated that President Truman wanted "a very thorough investigation" of the activities of the former official so that "steps might be taken, if possible, to see that [his] activities did not interfere with the proper administration of government." [111] The memorandum makes no reference to "subversive activities" or any other national security considerations.

The "Sugar Lobby" and Martin Luther King, Jr., wiretaps in the early 1960s both show the elasticity of the "domestic security" standard which supplemented President Roosevelt's "subversive activities" formulation. Among those wiretapped in the Sugar Lobby investigation, as noted above, was a Congressional staff aide. Yet the documentary record of this investigation reveals no evidence indicating that the target herself represented any threat to the "domestic security." Similarly, while the FBI may properly have been concerned with the activities of certain advisors to Dr. King, the direct wiretapping of Dr. King shows that the "domestic security" standard could be stretched to unjustified lengths.

The microphone surveillances of Congressman Cooley and Dr. King under the "national interest" standard established by Attorney General Brownell in 1954 also reveal the relative ease with which electronic bugging devices could be used against American citizens who

[107] See, e.g., *Olmstead* v. *United States*, 277 U.S. 438, (1928).
[108] Memorandum from Francis Biddle to Mr. Hoover, 11/19/41.
[109] Ibid.
[110] Unaddressed Memorandum from J. Edgar Hoover, 11/15/45, found in Director Hoover's "Official and Confidential" files.
[111] Ibid.

posed no genuine "national security" threat. Neither of these targets advocated or engaged in any conduct that was damaging to the security of the United States.

In April, 1964, Attorney General Robert Kennedy approved "technical coverage (electronic surveillance)" of a black nationalist leader after the FBI advised Kennedy that he was "forming a new group" which would be "more aggressive" and would "participate in racial demonstrations and civil rights activities." The only indication of possible danger noted in the FBI's request for the wiretaps, however, was that this leader had "recommended the possession of firearms by members for their self-protection."[112]

One year later, Attorney General Nicholas Katzenbach approved a wiretap on the offices of the Student Non-Violent Coordinating Committee on the basis of *potential* communist infiltration into that organization. The request which was sent to the Attorney General noted that "confidential informants" described SNCC as "the principal target for Communist Party infiltration among the various civil rights organizations" and stated that some of its leaders had "made public appearances with leaders of communist-front organizations" and had "subversive backgrounds."[113] The FBI presented no substantial evidence however, that SNCC was in fact infiltrated by communists—only that the organization was apparently a target for such infiltration in the future.

After the Justice Department adopted new criteria for the institution of warrantless electronic surveillance in 1968, the unjustified use of wiretaps continued. In November 1969, Attorney General John Mitchell approved a series of three wiretaps on organizations involved in planning the antiwar "March on Washington." The FBI's request for coverage of the first group made no claim that its members engaged or were likely to engage in violent activity; the request was simply based on the statement that the anticipated size of the demonstration was cause for "concern should violence of any type break out."[114]

The only additional justification given for the wiretap on one of the other groups, the Vietnam Moratorium Committee, was that it "has recently endorsed fully the activities of the [first group] concerning the upcoming antiwar demonstrations."[115]

In 1970, approval for a wiretap on a "New Left oriented campus group" was granted by Attorney General Mitchell on the basis of an FBI request which included, among other factors deemed relevant to the necessity for the wiretap, evidence that the group was attempting "to develop strong ties with the cafeteria, maintenance and other workers on campus" and wanted to "go into industry and factories and . . . take the radical politics they learned on the campus and spread them among factory workers."[116]

[112] Memorandum from J. Edgar Hoover to the Attorney General, 4/1/64.
[113] Memorandum from J. Edgar Hoover to the Attorney General, 6/15/65.
[114] Memorandum from J. Edgar Hoover to the Attorney General, 11/5/69.
[115] Memorandum from J. Edgar Hoover to Attorney General Mitchell, 11/7/69.
[116] Memorandum from J. Edgar Hoover to the Attorney General, 3/16/70. The strongest evidence that this group's conduct was inimical to the national security was reported as follows:

"The [group] is dominated and controlled by the pro-Chinese Marxist Leninist (excised). . . .

"In carrying out the Marxist-Leninist ideology of the (excised) members have repeatedly sought to become involved in labor disputes on the side of labor, join

This approval was renewed three months later despite the fact that the request for renewal made no mention of violent or illegal activity by the group. The value of the wiretap was shown, according to the FBI, by such results as obtaining "the identities of over 600 persons either in touch with the national headquarters or associated with" it during the preceding three months.[117] Six months after the original authorization the number of persons so identified had increased to 1,428; and approval was granted for a third three-month period."[118]

The "seventeen wiretaps" also show how the term "national security" as a justification for wiretapping can obscure improper use of this technique. Shortly after these wiretaps were revealed publicly, President Nixon stated they had been justified by the need to prevent leaks of classified information harmful to the national security.[119]

Wiretaps for this purpose had, in fact, been authorized under the Kennedy and Johnson administrations. President Nixon learned of these and other prior taps and, at a news conference, sought to justify the taps he had authorized by referring to past precedent. He stated that in the:

> period of 1961 to '63 there were wiretaps on news organizations, on news people, on civil rights leaders and on other people. And I think they were perfectly justified and I'm sure that President Kennedy and his brother, Robert Kennedy, would never have authorized them, unless he thought they were in the national interest. (Presidential News Conference, 8/22/73.)

Thus, questionable electronic surveillances by earlier administrations were put forward as a defense for improper surveillances exposed in 1973. In fact, however, two of these wiretaps were placed on domestic affairs advisers at the White House who had no foreign affairs responsibilities and apparently no access to classified foreign policy materials.[121] A third target was a White House speech writer who had been overheard on an existing tap agreeing to provide a reporter with background information on a Presidential speech con-

---

picket lines and engage in disruptive and sometimes violent tactics against industry recruiters on college campuses. . . .

"This faction is currently very active in many of the major demonstrations and student violence on college campuses. . . ." (Memorandum from J. Edgar Hoover to the Attorney General, 3/16/70. The excised words have been deleted by the FBI.)

[117] Memorandum from J. Edgar Hoover to the Attorney General, 6/16/70. The only other results noted by Hoover related to the fact that the wiretap had "obtained information concerning the activities of the national headquarters of [the group and] plans for [the group's] support and participation in demonstrations supporting antiwar groups and the (excised)." It was also noted that the wiretap "revealed . . . contacts with Canadian student elements".

[118] Memorandum from J. Edgar Hoover to the Attorney General, 9/16/70. The only other results noted by Hoover again related to obtaining information about the "plans and activities" of the group. Specifically mentioned were the "plans for the National Interim Committee (ruling body of [excised]) meeting which took place in New York and Chicago", and the plans "for demonstrations at San Francisco, Detroit, Salt Lake City, Minneapolis, and Chicago." There was no indication that these demonstrations were expected to be violent. (The excised words have been deleted by the FBI).

[119] Public statement of President Nixon, 5/22/73.

[121] Memorandum from J. Edgar Hoover to the Attorney General 7/23/69; memorandum from J. Edgar Hoover to the Attorney General 12/14/70.

94-628 O - 76 - 19

cerning domestic revenue sharing and welfare reform.[122] The reinstatement of another wiretap in this series was requested by H. R. Haldeman simply because "they may have a bad apple and have to get him out of the basket."[123] The last four requests in this series that were sent to the Attorney General (including the requests for a tap on the "bad apple") did not mention any national security justification at all. As former Deputy Attorney General William Ruckelshaus has testified:

> I think some of the individuals who were tapped, at least to the extent I have reviewed the record, had very little, if any, relationship to any claim of national security . . . I think that as the program proceeded and it became clear to those who could sign off on taps how easy it was to institute a wiretap under the present procedure that these kinds of considerations [i.e., genuine national security justifications] were considerably relaxed as the program went on.[124]

None of the "seventeen" wiretaps was ever reauthorized by the Attorney General, although 10 of them remained in operation for periods longer than 90 days and although President Nixon himself stated privately that "[t]he tapping was a very, very unproductive thing . . . it's never been useful to any operation I've conducted . . ."[125]

In short, warrantless electronic surveillance has been defended on the ground that it was essential for the national security, but the history of the use of this technique clearly shows that the imprecision and manipulation of this and similar labels, coupled with the absence of any outside scrutiny, has led to its improper use against American citizens who posed no criminal or national security threat to the country.[126]

Similarly, the terms "foreign intelligence" and "counterespionage" were used by the CIA and the FBI to justify their cooperation in the CIA's New York mail opening project, but this project was also used to target entirely innocent American citizens.

As noted above, the CIA compiled a "Watch List" of names of persons and organizations whose mail was to be opened if it passed through the New York facility. In the early days of the project, the names on this list—which then numbered fewer than twenty—might reason-

---

[122] Memorandum from W. C. Sullivan to C. D. DeLoach, 8/1/69.

[123] Memorandum from J. Edgar Hoover to Messrs. Tolson, Sullivan and D. C. Brennan, 10/15/70.

[124] Ruckelshaus testimony before the Senate Subcommittee on Administrative Practice and Procedure, 5/9/74, pp. 311–12.

[125] Transcript of the Presidential Tapes, 2/28/73 (House Judiciary Committee Statement of Information Book VII, Part W, p. 1754.)

[126] The term "national security" was also used by John Ehrlichman and Charles Colson to justify their roles in the break-in of Dr. Fielding's office in 1971. A March 21, 1973 tape recording of a meeting between President Nixon, John Dean, and H. R. Haldeman suggests, however, that the national security "justification" may have been developed long after the event for the purpose of obscuring its impropriety. When the President asked what could be done if the break-in was revealed publicly, John Dean suggested, "You might put it on a national security grounds basis." Later in the conversation, President Nixon stated "With the bombing thing coming out and everything coming out, the whole thing was national security," and Dean said, "I think we could get by on that." (Transcript of Presidential tapes, 3/21/73.)

ably have been expected to lead to genuine foreign intelligence or counterintelligence information. But as the project developed, the Watch List grew and its focus changed. By the late 1960s there were approximately 600 names on the list, many of them American citizens and organizations who were engaged in purely lawful and constitutionally protected forms of protest against governmental policies. Among the domestic organizations on the Watch List, which was supplemented by submissions from the FBI, were: Clergy and Laymen Concerned about Vietnam, the National Mobilization Committee to End the War in Vietnam, *Ramparts*, the Student Non-Violent Coordinating Committee, the Center for the Study of Public Policy, and the American Friends Service Committee.[127]

The FBI levied more general requirements on the CIA's project as well. The focus of the original categories of correspondence in which the FBI expressed an interest was clearly foreign counterespionage, but subsequent requirements became progressively more domestic in their focus and progressively broader in their scope. The requirements that were levied by the FBI in 1972, one year before the termination of the project, included the following:

> ". . . [p]ersons on the Watch List; known communists, New Left activists, extremists, and other subversives . . .
> Communist party and front organizations . . . extremist and New Left organizations.
> Protest and peace organizations, such as People's Coalition for Peace and Justice, National Peace Action Committee, and Women's Strike for Peace.
> Communists, Trotskyites and members of other Marxist-Leninist, subversive and extremist groups, such as the Black Nationalists and Liberation groups . . . Students for a Democratic Society . . . and other New Left groups.
> Traffic to and from Puerto Rico and the Virgin Islands showing anti-U.S. or subversive sympathies." [128]

This final set of requirements evidently reflected the domestic turmoil of the late 1960s and early 1970s. The mail opening program that began as a means of collecting foreign intelligence information and discovering Soviet intelligence efforts in the United States had expanded to encompass detection of the activities of domestic dissidents of all types.

. . . . . .

In the absence of effective outside control, highly intrusive techniques have been used to gather vast amounts of information about the entirely lawful activities—and privately held beliefs—of large numbers of American citizens. The very intrusiveness of these techniques demands the utmost circumspection in their use. But with vague or non-existent standards to guide them, and with labels such as "national security" and "foreign intelligence" to shield them, executive branch officials have been all too willing to unleash these techniques against American citizens with little or no legitimate justification.

[127] Staff summary of Watch List review, 9/5/75.
[128] Routing slip from J. Edgar Hoover to James Angelton (attachment), 3/10/72.

APPENDIX E

E. POLITICAL ABUSE OF INTELLIGENCE INFORMATION

Major Finding

The Committee finds that information has been collected and disseminated in order to serve the purely political interests of an intelligence agency or the administration, and to influence social policy and political action.

Subfindings

(a) White House officials have requested and obtained politically useful information from the FBI, including information on the activities of political opponents or critics.

(b) In some cases, political or personal information was not specifically requested, but was nevertheless collected and disseminated to administration officials as part of investigations they had requested. Neither the FBI nor the recipients differentiated in these cases between national security or law enforcement information and purely political intelligence.

(c) The FBI has also volunteered information to Presidents and their staffs, without having been asked for it, sometimes apparently to curry favor with the current administration. Similarly, the FBI has assembled intelligence on its critics and on political figures it believed might influence public attitudes or Congressional support.

(d) The FBI has also used intelligence as a vehicle for covert efforts to influence social policy and political action.

Elaboration of Findings

The FBI's ability to gather information without effective restraints gave it enormous power. That power was inevitably attractive to politicians, who could use information on opponents and critics for their own advantage, and was also an asset to the Bureau, which depended on politicians for support. In the political arena, as in other facets of American life touched by the intelligence community, the existence of unchecked power led to its abuse.

By providing politically useful information to the White House and congressional supporters, sometimes on demand and sometimes gratuitously, the Bureau buttressed its own position in the political structure. At the same time, the widespread—and accurate—belief in Congress and the administration that the Bureau had available to it, derogatory information on politicians and critics created what the late Majority Leader of the House of Representatives, Hale Boggs, called a "fear" of the Bureau:

> Freedom of speech, freedom of thought, freedom of action for men in public life can be compromised quite as effectively by the fear of surveillance as by the fact of surveillance.[1]

[1] Remarks by Rep. Hale Boggs, 4/22/71, Congressional Record, Vol. 117, Part 9, p. 11565.

Information gathered and disseminated to the White House ranged from purely political intelligence, such as lobbying efforts on bills an administration opposed and the strategy of a delegate challenge at a national political convention, to "tidbits" about the activities of politicians and public figures which the Bureau believed "of interest" to the recipients.

Such participation in political machinations by an intelligence agency is totally improper. Responsibility for what amounted to a betrayal of the public trust in the integrity of the FBI must be shared between the officials who requested such information and those who provided it.

The Bureau's collection and dissemination of politically useful information was not colored by partisan considerations; rather its effect was to entrench the Bureau's own position in the political structure, regardless of which party was in power at the time. However, the Bureau also used its powers to serve ideological purposes, attempting covertly to influence social policy and political action.

In its efforts to "protect society," the FBI engaged in activities which necessarily affected the processes by which American citizens make decisions. In doing so, it distorted and exaggerated facts, made use of the mass media, and attacked the leadership of groups which it considered threats to the social order.

Law enforcement officers are, of course, entitled to state their opinions about what choices the people should make on contemporary social and political issues. The First Amendment guarantees their right to enter the marketplace of ideas and persuade their fellow citizens of the correctness of those opinions by making speeches, writing books, and, within certain statutory limits, supporting political candidates. The problem lies not in the open expression of views, but in the covert use of power or position of trust to influence others. This abuse is aggravated by the agency's control over information on which the public and its elected representatives rely to make decisions.

The essence of democracy is the belief that the people must be free to make decisions about matters of public policy. The FBI's actions interfered with the democratic process, because attitudes within the Bureau toward social change led to the belief that such intervention formed a part of its obligation to protect society. When a governmental agency clandestinely tries to impose its views of what is right upon the American people, then the democratic process is undermined.

Subfinding (a)

White House officials have requested and obtained politically useful information from the FBI, including personal life information on the activities of political opponents or critics.

Presidents and White House aides have asked the FBI to provide political or personal information on opponents and critics, including "name checks" of Bureau files.[2] They have also asked the Bureau to

[2] A "name check" is not an investigation, but a search of existing FBI files through the use of the Bureau's comprehensive general name index. Requests for FBI "name checks" were peculiarly damaging because no new investigation was done to verify allegations stored away for years in Bureau files. A former FBI official responsible for compliance with such requests said that the Bureau "answered . . . by furnishing the White House every piece of information in our files on the individuals requested." Deposition of Thomas E. Bishop, former Assistant Director, Crime Records Division, 12/2/75, p. 144.)

conduct electronic surveillance or more limited investigations of such persons. The FBI appears to have complied unquestioningly with these requests, despite occasional internal doubts about their propriety.[3]

Precedents for certain political abuses go back to the very outset of the domestic intelligence program. In 1940 the FBI complied with President Roosevelt's request to file the names of people sending critical telegrams to the White House.[4] There is evidence of improper electronic surveillance for the White House in the 1940s.[5] And an aide to President Eisenhower asked the FBI to conduct a questionable name check.[6] In 1962, the FBI complied unquestioningly with a request from Attorney General Kennedy to interview a steel executive and several reporters who had written stories about a statement by the executive.[7] As part of an investigation of foreign lobbying efforts on sugar quota legislation in 1961 and 1962, Attorney General Kennedy requested wiretaps on a Congressional aide, three executive officials, and two American lobbyists, including a Washington law firm.[8]

Nevertheless, the political misuse of the FBI under the Johnson and Nixon administrations appears to have been more extensive than in previous years.

Under the Johnson administration, the FBI was used to gather and report political intelligence on the administration's partisan opponents in the last days of the 1964 and 1968 Presidential election

---

[3] Former FBI executive Cartha DeLoach, who was FBI liaison with the White House during part of the Johnson administration, has stated, "I simply followed Mr. Hoover's instructions in complying with White House requests and I never asked any questions of the White House as to what they did with the material afterwards." (DeLoach deposition, 11/25/75, p. 28.) On at least one occasion, when a White House aide indicated that President Johnson did not want any record made by the FBI of a request for a "run-down" on the links between Robert Kennedy and officials involved in the Bobby Baker investigation, the Bureau disregarded the order. DeLoach stated that he "ignored the specific instructions" in this instance because he "felt that any instructions we received from the White House should be a matter of record." (DeLoach deposition, 11/25/75, p. 89.)

Former Assistant Director Bishop stated, "Who am I to ask the President of the United States what statutory basis he has if he wants to know what information is in the files of the FBI?" It was a "proper dissemination" because it was "not a dissemination outside the executive branch" and because there was "no law, no policy of the Department of Justice, . . . no statute of the United States that says that was not permissible." But even if there had been a statute laying down standards, Bishop said "it wouldn't have made a bit of difference . . . when the Attorney General or the President asks for it."

Bishop recalled from his "own knowledge" instances where President Kennedy, Johnson, and Nixon had "called over and asked Mr. Hoover for a memo on certain people." (Bishop deposition, 12/2/75, pp. 153–154.)

[4] Memoranda from Stephen Early, Secretary to the President, to Hoover, 5/21/40 and 6/17/40.

[5] FBI memorandum to Senate Select Committee, 3/26/76; See pp. 36–37.

[6] Memorandum from J. Edgar Hoover to Thomas E. Stephens, Secretary to the President, 4/13/54.

[7] Courtney Evans deposition, 12/1/75, p. 39.

[8] See pp. 64–65. The tap authorized by Attorney General Kennedy on another high executive official was not related to political considerations, nor apparently was the tap authorized by Attorney General Katzenbach in 1965 on the editor of an anti-communist newsletter who had published a book alleging impropriety by Robert Kennedy a year earlier.

campaigns. In the closing days of the 1964 campaign, Presidential aide Bill Moyers asked the Bureau to conduct "name checks" on all persons employed in Senator Goldwater's Senate office, and information on two staff members was reported to the White House.[9] Similarly, in the last two weeks of the 1968 campaign, the Johnson White House requested an investigation (including indirect electronic surveillance and direct physical surveillance) of Mrs. Anna Chennault, a prominent Republican leader, and her relationships with certain South Vietnamese officials.[10] This investigation also included an FBI check of Vice Presidential candidate Spiro Agnew's long distance telephone call records, apparently at the personal request of President Johnson.[11]

Another investigation for the Johnson White House involved executive branch officials who took part in the criminal investigation of former Johnson Senate aide Bobby Baker. When Baker's trial began in 1967, it was revealed that one of the government witnesses had been "wired" to record his conversations with Baker. Presidential aide Marvin Watson told the FBI that Johnson was quite "exercised," and the Bureau was ordered to conduct a discreet "run-down" on the former head of the Justice Department's Criminal Division and four Treasury Department officials who had been responsible for "wiring"

[9] Memorandum from Hoover to Moyers, 10/27/64, cited in FBI summary memorandum, 1/31/75.

[10] Bureau files indicate that the apparent "reason" for the "White House interest" was to determine "whether the South Vietnamese had secretly been in touch with supporters of Presidential candidate Nixon, possibly through Mrs. Chennault, as President Johnson was apparently suspicious that the South Vietnamese were trying to sabotage his peace negotiations in the hope that Nixon would win the election and then take a harder line towards North Vietnam." (FBI memorandum, subject: Mrs. Anna Chennault, 2/1/75.) The FBI has claimed that its investigation of Mrs. Chennault was "consistent with FBI responsibilities to determine if her activities were in violation of certain provisions of the Foreign Agents Registration Act and of the Neutrality Act."

Direct electronic surveillance of Mrs. Chennault was rejected, according to a contemporaneous FBI memorandum, because FBI executive Cartha DeLoach pointed out that "it was widely known that she was involved in Republican political circles and, if it became known that the FBI was surveilling her this would put us in a most untenable and embarrassing position." (Memorandum from DeLoach to Tolson, 10/30/68.)

Electronic surveillance was, however, directed at the South Vietnamese officials and was approved by Attorney General Ramsey Clark. Clark has testified that he did not know of the physical surveillance aspect of the FBI's investigation, but that he did authorize the electronic surveillance of the South Vietnamese officials. (Clark testimony, 12/3/75, Hearings, Vol. 6, p. 252.)

[11] FBI executive Cartha DeLoach has stated that a White House aide made the initial request for the check of telephone company records late one night. According to DeLoach, the request was "to find out who, either Mr. Agnew or Mr. Nixon, when they had been in Albuquerque (New Mexico) several days prior to that, had called from Albuquerque while they were there." When DeLoach refused to contact the telephone company "late in the evening," President Johnson "came on the phone and proceeded to remind me that he was Commander in Chief and he should get what he wanted, and he wanted me to do it immediately." DeLoach then talked with Director Hoover, who told him to "stand your ground." The next day, however, Hoover ordered that the records be checked, but the only calls identified were "made by Mr. Agnew's staff." These were reported to the White House. (DeLoach Deposition, 11/25/75, pp. 74–75.) Agnew's arrival and departure times in and out of Albuquerque were also "verified at the request of the White House." (FBI summary memorandum, subject: Mrs. Anna Chennault, 2/1/75).

the witness. The Bureau was specifically insisted to include any associations between those persons and Robert Kennedy.[12]

Several Johnson White House requests were directed at critics of the war in Vietnam, at newsmen, and at other opponents. According to a Bureau memorandum, White House aide Marvin Watson attempted to disguise his, and the President's interest in such requests by asking the FBI to channel its replies through a lower level White House staff member.[13]

In 1966, Watson asked the FBI to monitor the televised hearings of the Senate Foreign Relations Committee on Vietnam policy and prepare a memorandum comparing statements of the President's Senate critics with "the Communist Party line." [14] Similarly, in 1967 when seven Senators made statements criticizing the bombing of North Vietnam, Watson requested (and the Bureau delivered) a "blind memorandum" setting forth information from FBI files on each of the Senators. Among the data supplied were the following items:

> Senator Clark was quoted in the press as stating that the three major threats to America are the military-industrial complex, the Federal Bureau of Investigation, and the Central Intelligence Agency.
>
> Senator McGovern spoke at a rally sponsored by the Chicago Committee for a Sane Nuclear Policy, a pacifist group. Senator McGovern stated that the "United States was making too much of the communist take-over of Cuba."
>
> [Another Senator now deceased] has, on many occasions, publicly criticized United States policy toward Vietnam. He frequently speaks before groups throughout the United States on this subject. He has been reported as intentionally entering into controversial areas so that his services as a speaker for which he receives a fee, will be in demand.[15]

The Johnson administration also requested information on contacts between members of Congress and certain foreign officials known to oppose the United States presence in Vietnam. According to FBI

[12] FBI Director Hoover brought the matter to the attention of the White House in a letter describing why the FBI had refused to "wire" the witness (there was not adequate "security") and how the Criminal Division had then used the Bureau of Narcotics to do so. (Memorandum from Hoover to Watson, 1/12/67.) This was the instance where FBI executive Cartha DeLoach made a record, after Watson told him that "the President does not want any record made." (Memorandum from DeLoach to Tolson, 1/17/67; see also FBI summary memorandum, 2/3/75.)

[13] According to this memorandum, Watson told Cartha DeLoach in 1967 that "he and the President" wanted all "communications addressed to him by the Director" to be addressed instead to a lower level White House staff member. Watson told DeLoach that the "reason for this change" was that the staff member "did not have the direct connection with the President that he had and, consequently, people who saw such communications would not suspicion (sic) that Watson or the President had requested such information, nor were interested in such information." (Memorandum from De Loach to Tolson, 3/17/67.)

[14] FBI summary memorandum, subject: Coverage of Television Presentation. Senate Foreign Relations Committee, 1/31/75. Former FBI executive Cartha DeLoach has stated, regarding this incident, "We felt that it was beyond the jurisdiction of the FBI, but obviously Mr. Hoover felt that this was a request by the President and he desired it to be done." (DeLoach deposition, 11/25/75, p. 58.)

[15] Blind FBI memorandum, 2/10/67.

records, President Johnson believed these foreign officials had generated "much of the protest concerning his Vietnam policy, particularly the hearings in the Senate." [16]

White House requests were not limited to critical Congressmen. Ordinary citizens who sent telegrams protesting the Vietnam war to the White House were also the subject of Watson requests for FBI name check reports.[17] Presidential aide Jake Jacobsen asked for name checks on persons whose names appeared in the Congressional Record as signers of a letter to Senator Wayne Morse expressing support for his criticism of U.S. Vietnam policy.[18] On at least one occasion, a request was channeled through Attorney General Ramsey Clark, who supplied Watson (at the latter's request) with a summary of information on the National Committee for a Sane Nuclear Policy.[19]

Other individuals who were the subject of such name check requests under the Johnson Administration included NBC Commentator David Brinkley,[20] Associated Press reporter Peter Arnett,[21] columnist Joseph Kraft,[22] Life magazine Washington bureau chief Richard Stolley,[23] Chiago Daily News Washington bureau chief Peter Lisagor,[24] and Ben W. Gilbert of the Washington Post.[25] The Johnson White House also requested (and received) name check reports on the authors of books critical of the Warren Commission report; some of these reports included derogatory information about the personal lives of the individuals.[26]

The Nixon administration continued the practice of using the FBI to produce political information. In 1969 John Ehrlichman, counsel to President Nixon, asked the FBI to conduct a "name check" on Joseph Duffy, chairman of Americans for Democratic Action. Data in Bureau files covered Duffy's "handling arrangements" for an anti-war teach-in in 1965, his position as State Coordinator of the group

[16] President Johnson's request also went beyond "legislators," and included contacts by any "prominent U.S. citizens." (FBI summary memorandum, subject: Information Concerning Contacts Between [Certain Foreign officials] and Members or Staff of the United States Congress Furnished to the White House at the Request of the President, 2/3/75.) The FBI's reports indicated that its information came "through coverage" of the foreign officials and that the Bureau, in this case, had "conducted no investigation of members of Congress." (FBI summary memorandum, 2/3/75.) FBI "coverage" apparently included electronic surveillance.

President Nixon also requested information on contacts between foreign officials and Congressmen, but his request does not appear to have related to Presidential critics. Rather, the Nixon request grew out of concern about "an increase in [foreign] interest on Capitol Hill" which had been expressed to President Nixon by at least one Senator; and the FBI's report "included two examples of [foreign] intelligence initiatives directed against Capitol Hill without identifying the [forelgners] or American involved." (FBI summary memorandum, 2/3/75.)

[17] Memoranda from Hoover to Watson, 6/4/65 and 7/30/65.

[18] Memorandum from Hoover to Watson, 7/15/66, citing Jacobsen request.

[19] Memorandum from Clark to Watson, 4/8/67, enclosing memorandum from Director, FBI to the Attorney General, 4/7/67. (LBJ Library.)

[20] Memoranda from Hoover to Watson, 2/15/65 and 5/29/65.

[21] Memorandum from Hoover to Watson, 7/22/65.

[22] Memorandum from Hoover to Watson, 1/27/67.

[23] Memorandum from Hoover to Watson, 4/6/66.

[24] Memorandum from Hoover to Watson, 2/24/66.

[25] Memorandum from Hoover to Watson, 4/6/66.

[26] Memorandum from Hoover to Watson, 11/8/66; DeLoach, 12/3/75, Hearings, Vol. 6, pp. 180–182.

"Negotiation Now" in 1967, and his activity as chairman of Connecticut Citizens for McCarthy in 1968.[26a]

Presidential aide H. R. Haldeman requested a name check on CBS reporter Daniel Schorr. In this instance, the FBI mistakenly considered the request to be for a full background investigation and began to conduct interviews. These interviews made the inquiry public. Subsequently, White House officials stated (falsely) that Schorr was under consideration for an executive appointment.[27] In another case, a Bureau memorandum states that Vice President Agnew asked the FBI for information about Rev. Ralph David Abernathy, then head of the Southern Christian Leadership Conference, for use in "destroying Abernathy's credibility." [28] (Agnew has denied that he made such a request, but agrees that he received the information.)[29]

Several White House requests involved the initiation of electronic surveillance. Apparently on the instructions of President Nixon's aide John Ehrlichman and Director Hoover, FBI Assistant Director William C. Sullivan arranged for the microphone surveillance of the hotel room of columnist Joseph Kraft while he was visiting a foreign country.[30] Kraft was also the target of physical surveillance by the FBI.[31] There is no record of any specific "national security" rationale for the surveillance.

Similarly, although the "17" wiretaps were authorized ostensibly to investigate national security "leaks," there is no record in three of the cases of any national security claim having been advanced in their support. Two of the targets were domestic affairs advisers at the White House, with no foreign affairs duties and no access to foreign policy materials.[32] A third was a White House speechwriter who had been overheard on an existing tap agreeing to provide a reporter with background on a presidential speech concerning, not foreign policy, but revenue sharing and welfare reform.[33]

[26a] Letter from J. Edgar Hoover to John D. Ehrlichman, 10/6/69; letter from Clarence M. Kelly to Joseph Duffy, 7/14/75, enclosing FBI records transmitted under Freedom of Information Act.

[27] House Judiciary Committee Hearings, Book VII, White House Surveillance Activities (1974), p. 1111.

[28] According to Director Hoover's memorandum of the conversation, Agnew asked Hoover for "some assistance" in obtaining information about Rev. Abernathy. Hoover recorded: "The Vice President said he thought he was going to have to start destroying Abernathy's credibility, so anything I can give him would be appreciated. I told him I would be glad to." (Memorandum from Hoover to Tolson, et al. 5/18/70.) Subsequently, the FBI Director sent Agnew a report on Rev. Abernathy containing not only the by-product of Bureau investigations, but also derogatory public record information. (Letter from Hoover to Agnew, 5/19/70.)

[29] Staff summary of Spiro Agnew interview, 10/15/75.

[30] Memoranda from Sullivan to Hoover, 6/30/69 and 7/2/69.

[31] Memorandum from Sullivan to DeLoach, 11/5/69. The Kraft surveillance is also discussed in Part II, pp. 121–122.

[32] Coverage in these two cases was requested by neither Henry Kissinger nor Alexander Haig (as most of the "17" were), but by other White House officials. Attorney General Mitchell approved the first at the request of "higher authority." (Memorandum from Hoover to Mitchell, 7/23/69.) The second was specifically requested by H. R. Haldeman. (Memorandum from Hoover to Mitchell, 12/14/70.

[33] This tap was also apparently requested by White House officials other than Kissinger or Haig. (Memorandum from Sullivan to DeLoach, 8/1/69.) The "17" wiretaps are also discussed at p. 122.

Subfinding (b)

In some cases, political or personal information was not specifically requested, but was nevertheless collected and disseminated to administration officials as part of investigations they had requested. Neither the FBI nor the recipients differentiated in these cases between national security or law enforcement information and purely political intelligence.

In some instances, the initial request for or dissemination of information was premised upon law enforcement or national security purposes. However, pursuant to such a request, information was furnished which obviously could serve only partisan or personal interests. As one Bureau official summarized its attitude, the FBI "did not decide what was political or what represented potential strife and violence. We are an investigative agency and we passed on all data." [34]

Examples from the Eisenhower, Kennedy, Johnson, and Nixon administrations illustrate this failure to distinguish between political and nonpolitical intelligence. They include the FBI's reports to the White House in 1956 on NAACP lobbying activities, the intelligence about the legislative process produced by the "sugar lobby" wiretaps in 1961–1962, the purely political data disseminated to the White House on the credentials challenge in the 1964 Democratic Convention, and dissemination of both political and personal information from the "leak" wiretaps in 1969–1972.

(i) The NAACP

In early 1956 Director Hoover sent the White House a memorandum describing the "potential for violence" in the current "racial situation".[35] Later reports to the White House, however, went far beyond intelligence about possible violence; they included extensive inside information about NAACP lobbying efforts, such as the following:

> A report on "meetings held in Chicago" in connection with a planned Leadership Conference on Civil Rights to be held in Washington under the sponsorship of the NAACP.[36]
>
> An extensive report on the Leadership Conference, based on the Bureau's "reliable sources" and describing plans of Conference delegations to visit Senators Paul Douglas, Herbert Lehman, Wayne Morse, Hubert Humphrey, and John Bricker. The report also summarized a speech by Roy Wilkins, other conference proceedings, and the report of "an informant" that the United Auto Workers was a "predominant organization" at the conference.[37]
>
> Another report on the conference included an account of what transpired at meetings between conference delegations and Senators Paul Douglas and Everett Dirksen.[38]

---

[34] DeLoach, 12/3/75, Hearings, Vol. 6, p. 180.

[35] Memorandum from Hoover to Dillon Anderson, Special Assistant to the President, 1/3/56. This report was also provided to the Attorney General, the Secretary of Defense, and military intelligence.

[36] Memorandum from Hoover to Anderson, 3/2/56.

[37] Memorandum from Hoover to Anderson, 3/5/56.

[38] Memorandum from Hoover to Anderson, 3/6/56.

A report including the information that two New Jersey congressmen would sign a petition to the Attorney General.[39]

A presidential aide suggested that Hoover brief the Cabinet on "developments in the South." [40] Director Hoover's Cabinet briefing also included political intelligence. He covered not only the NAACP conference, but also the speeches and political activities of Southern Senators and Governors and the formation of the Federation for Constitutional Government with Southern Congressmen and Governors on its advisory board.[41]

(*ii*) *The Sugar Lobby*

The electronic surveillance of persons involved in a foreign country's lobbying activities on sugar quota legislation in 1961–1962, authorized by Attorney General Robert Kennedy for the White House, also produced substantial political intelligence unrelated to the activities of foreign officials.[42] Such information came from wiretaps both on foreign officials and on American citizens, as well as from the microphone surveillance of the chairman of the House Agriculture Committee when he met with foreign officials in a New York hotel room.[43] The following are examples of the purely political (and personal) by-product:

A particular lobbyist "mentioned he is working on the Senate and has the Republicans all lined up." [44]

The same lobbyist said that "he had seen two additional representatives on the House Agriculture Committee, one of

---

[39] Memorandum from Hoover to Anderson, 3/7/56. A National Security Council staff member responsible for internal security matters summarized these reports as providing information "regarding attempts being made by the National Association for the Advancement of Colored People to send instructed delegations to high-ranking Government officials 'to tactfully draw out their positions concerning civil rights.'" (Memorandum from J. Patrick Coyne to Anderson, 3/6/56.)

[40] After consulting the Attorney General, this aide advised the Secretary to the Cabinet that the FBI had "reported developments in recent weeks in several southern States, indicating a marked deterioration in relationships between the races, and in some instances fomented by communist or communist-front organizations." (Memorandum from Anderson to Maxwell Rabb, 1/16/56.) The Secretary to the Cabinet, who had "experience in handling minority matters" for the White House, agreed that "each Cabinet Member should be equipped with the plain facts." (Memorandum from Rabb to Anderson, 1/17/56.) A National Security Council staff member who handled internal security matters reported shortly thereafter that the FBI Director was "prepared to brief the Cabinet along the general lines" of his written communications to the White House. (Memorandum from J. Patrick Coyne to Anderson, 2/1/56.)

[41] Memorandum from Director, FBI, to the Executive Assistant to the Attorney General, 3/9/56, enclosing FBI memorandum described as the "basic statement" used by the Director "in the Cabinet Briefing this morning on Racial Tension and Civil Rights." For a further discussion of the exaggeration of Communist influence on the NAACP in this briefing, see pp. 250–257, note 151a.

[42] The electronic surveillances were generally related to foreign affairs concerns. See pp. 64–65.

[43] The Americans include three Agriculture Department officials, the secretary to the Chairman of the House Agriculture Committee, and two registered lobbying agents for foreign interests. For Attorney General Kennedy's relationship to the microphone surveillance of the Congressman, see p. 61, note 233. One of the wiretaps directed at a registered lobbying agent was placed on the office telephone of a Washington law firm. (See p. 201)

[44] FBI memorandum, 6/15/62.

whom was 'dead set against us' and who may reconsider, and the other was neutral and 'may vote for us.' "[45]

The Agriculture Committee chairman believed "he had accomplished nothing" and that "he had been fighting over the Rules Committee and this had interfered with his attempt to organize."[46]

The "friend" of a foreign official "was under strong pressure from the present administration, and since the 'friend' is a Democrat, it would be very difficult for him to present a strong front to a Democratic Administration."[47]

A lobbyist stated that Secretary of State Rusk "had received a friendly reception by the Committee and there appeared to be no problem with regard to the sugar bill."[48]

A foreign official was reported to be in contact with two Congressmen's secretaries "for reasons other than business." The official asked one of the secretaries to tell the other that he "would not be able to call her that evening" and that one of his associates "was planning to take [the two secretaries and another Congressional aide] to Bermuda."[49]

The FBI's own evaluation of these wiretaps indicates that they "undoubtedly . . . contributed heavily to the Administration's success" in passing the legislation it desired.[50]

(iii) The 1964 Democratic Convention

Political reports were disseminated by the FBI to the White House from the 1964 Democratic convention in Atlantic City. These reports, from the FBI's "special squad" at the convention, apparently resulted from a civil disorders intelligence investigation which got out of hand because no one was willing to shut off the partisan by-product.[51] They centered on the Mississippi Freedom Democratic Party's credentials challenge. Examples of the political intelligence which flowed from FBI surveillance at the 1964 convention include the following:[52]

---

[45] FBI memorandum, 6/15/62.

[46] Memorandum from Hoover to Attorney General Kennedy, 2/18/61. This information came from the Bureau's "coverage" (by microphone surveillance) of the Congressman's hotel room meeting.

[47] FBI memorandum, 2/15/62.

[48] Memorandum from J. Edgar Hoover to Robert Kennedy, 3/13/61.

[49] Memorandum from J. Edgar Hoover to Robert Kennedy, 3/13/61.

[50] Memorandum from W. R. Wannall to W. C. Sullivan, 12/22/66. According to a Bureau memorandum of a meeting between Attorney General Kennedy and FBI Assistant Director Courtney Evans, Kennedy stated in April 1961 that "now the law has passed he did not feel there was justification for continuing this extensive investigation." (Memorandum from Evans to Parsons, 4/15/61.)

[51] There is no clear evidence as to what President Johnson had in mind when, as a contemporaneous FBI memorandum indicates, he directed "the assignment of the special squad to Atlantic City." (DeLoach to Mohr, 8/29/64) Cartha DeLoach has testified that Presidential aide Walter Jenkins made the original request to him, but that he said it should be discussed with Director Hoover and that "Mr. Jenkins or the President, to the best of my recollection, later called Mr. Hoover and asked that this be done." DeLoach claimed that the purpose was to gather "intelligence concerning matters of strife, violence, etc." which might arise out of the credentials challenge. (DeLoach, 12/3/75, hearings, Vol. 6, p. 175.)

[52] The operations of the FBI in Atlantic City are described in greater detail in Section II, pp. 117–119.

Dr. Martin Luther King and an associate "were drafting a telegram to President Johnson . . . to register a mild protest. According to King, the President pledged complete neutrality regarding the selecting of the proper Mississippi delegation to be seated at the convention. King feels that the Credentials Committee will turn down the Mississippi Freedom Party and that they are doing this because the President exerted pressure on the committee along this line." [53]

Another associate of Dr. King contacted a member of the MFDP who "said she thought King should see Governor Endicott Peabody of Massachusetts, Mayor Robert Wagner of New York City, Governor Edmund G. (Pat) Brown of California, Mayor Richard Daley of Chicago, and Governor John W. King of New Hampshire." The purpose was "to urge them to call the White House directly and put pressure on the White House in behalf of the MFDP." [54]

"MFDP leaders have asked Reverend King to call Governor Egan of Alaska and Governor Burns of Hawaii in an attempt to enlist their support. According to the MFDP spokesman, the Negro Mississippi Party needs these two states plus California and New York for the roll call tonight." [55]

An SCLC staff member told a representative of the MFDP: "Off the record, of course, you know we will accept the Green compromise proposed." This referred to "the proposal of Congresswoman Edith Green of Oregon." [56]

In a discussion between Dr. King and another civil rights leader, the question of "a Vice-Presidential nominee came up and King asked what [the other leader] thought of Hugh [sic] Humphrey, and [the other leader] said Hugh Humphrey is not going to get it, that Johnson needs a Catholic . . . and therefore the Vice President will be Muskie of Maine." [57]

An unsigned White House memorandum disclosing Dr. King's strategy in connection with a meeting to be attended by President Johnson suggests that there was political use of these FBI reports.[58]

(iv) The "17" Wiretaps.

The Nixon White House learned a substantial amount of purely political intelligence from wiretaps to investigate "leaks" of classified information placed on three newsmen and fourteen executive officials during 1969–1971.[59] The following illustrate the range of data supplied:

One of the targets "recently stated that he was to spend an hour with Senator Kennedy's Vietnam man, as Senator Kennedy is giving a speech on the 15th." [60]

[53] Memorandum from DeLoach to Jenkins, 8/24/64.
[54] Memorandum from DeLoach to Jenkins, 8/25/64.
[55] Memorandum from DeLoach to Jenkins, 8/25/64.
[56] Memorandum rom DeLoach to Jenkins, 8/25/64.
[57] Memorandum from DeLoach to Jenkins, 8/25/64.
[58] Blind memorandum from LBJ Library bearing handwritten date 8/26/64 and the typewritten date 8/19/64, Hearings, Vol. 6, Exhibit 68–2, p. 713.
[59] In at least two instances, the wiretaps continued on targets after they left the Executive Branch and became advisers to Senator Edmund Muskie, then the leading Democratic prospect for the Presidency. See Part II, p. 122.
[60] Memorandum from Hoover to Nixon, Kissinger, and Mitchell, 10/9/69.

Another target said that Senator Fulbright postponed congressional hearings on Vietnam because he did not believe they would be popular at that time.[61]

A well-known television news correspondent "was very distressed over having been 'singled out' by the Vice President." [62]

A friend of one of the targets said the *Washington Star* planned to do an article critical of Henry Kissinger.[63]

One of the targets helped former Ambassador Sargent Shriver write a press release criticizing a recent speech by President Nixon in which the President "attacked" certain Congressmen.[64]

One of the targets told a friend it "is clear the Administration will win on the ABM by a two-vote margin. He said 'They've got [a Senator] and they've got [another Senator].'." [65]

A friend of one of the targets wanted to see if a Senator would "buy a new amendment" and stated that "they" were "going to meet with" another Senator.[66]

A friend of one of the targets described a Senator as "marginal" on the Cooper-Church Amendment and stated that another Senator might be persuaded to support it.[67]

One of the targets said Senator Mondale was in a "dilemma" over the "trade bill." [68]

A friend of one of the targets said he had spoken to former President Johnson and "Johnson would not back Senator Muskie for the Presidency as he intended to stay out of politics." [69]

There is at least one clear example of the political use of such information. After the FBI Director informed the White House that former Secretary of Defense Clark Clifford planned to write a magazine article criticizing President Nixon's Vietnam policy,[70] White House aide Jeb Stuart Magruder advised John Ehrlichman and H. R. Haldeman that "we are in a position to counteract this article in any number of ways." [71] It is also significant that, after May 1970, the FBI Director's letters summarizing the results of the wiretaps were no longer sent to Henry Kissinger, the President's national security advisor, but to the President's political advisor, H. R. Haldeman.[72]

. . . . . .

[61] Memorandum from Hoover to Nixon and Kissinger, 12/3/69.
[62] Memorandum from Hoover to Nixon and Kissinger, 2/26/70.
[63] Memorandum from Hoover to H. R. Haldeman, 6/2/70.
[64] Memorandum from Hoover to Haldeman. 9/4/70.
[65] Memorandum from Hoover to Nixon and Kissinger, 7/18/69.
[66] Memorandum from Hoover to Haldeman, 5/18/70.
[67] Memorandum from Hoover to Haldeman, 6/23/70.
[68] Memorandum from Hoover to Haldeman, 11/24/70.
[69] Memorandum from Hoover to Haldeman, 12/22/70.
[70] Memorandum from Hoover to Nixon, Kissinger, and Mitchell, 12/29/69.
[71] Memorandum from Magruder to Haldeman and Ehrlichman, 1/15/70. Ehrlichman advised Haldeman, "This is the kind of early warning we need more of—your game planners are now in an excellent position to map anticipatory action." (Memorandum from "E" (Ehrlichman) to "H" (Haldeman), undated.) Haldeman responded, "I agree with John's point. Let's get going." (Memorandum from "H" to "M" (Magruder), undated).
[72] Report of the House Judiciary Committee, 8/20/74, p. 147.

These four illustrations from administrations of both political parties indicate clearly that direct channels of communication between top FBI officials and the White House, combined with the failure to screen out extraneous information, and coupled with overly broad investigations in the first instance, have been sources of flagrant political abuse of the intelligence process.[73]

Subfinding (c)

The FBI has also volunteered information to Presidents and their staffs, without having been asked for it, sometimes apparently to curry favor with the current administration. Similarly, the FBI has assembled information on its critics and on political figures it believed might influence public attitudes or Congressional support.

There have been numerous instances over the past three decades where the FBI volunteered to its superiors purely political or personal information believed by the FBI Director to be "of interest" to them.[74]

The following are examples of the information in Director Hoover's letters under the Truman, Eisenhower, Kennedy, and Johnson administrations.[75]

> To Major General Harry Vaughn, Military Aide to President Truman, a report on the activities of a former Roosevelt aide who was trying to influence the Truman administration's appointments.[76]
>
> To Matthew J. Connelly, Secretary to President Truman, a report from a "very confidential source" about a meeting of newspaper representatives in Chicago to plan publication of stories exposing organized crime and corrupt politicians.[77]
>
> To Dillon Anderson, Special Assistant to President Eisenhower, the advance text of a speech to be delivered by a prominent labor leader.[78]

---

[73] It should be noted, however, that in at least one case the Bureau did distinguish between political and non-political information. In 1968, when an aide to Vice President Humphrey asked that a "special squad" be sent to the Democratic National Convention in Chicago, Director Hoover not only declined, but he also specifically instructed the SAC in Chicago not "to get into anything political" but to confine his reports to "extreme action or violence." (Memorandum from Hoover to Tolson., et al, 8/15/68.) There were no comparable instructions at Atlantic City.

[74] Former Attorney General Francis Biddle recalled in his autobiography how J. Edgar Hoover shared with him some of the "intimate details" of what his fellow Cabinet members did and said, "their likes and dislikes, their weaknesses and their associations." Biddle confessed that he enjoyed hearing these derogatory and sometimes "embarrassing" tidbits and that Hoover "knew how to flatter his superior." (Francis Biddle, *In Brief Authority* [Garden City: Doubleday, 1962], pp. 258–259.)

A former FBI official has described one aspect of the Bureau's practice:

"Mr. Hoover would say what do we have in our files on this guy? Just what do we have? Not blind memorandum, not public source information, everything we've got. And we would maybe write a 25 page memo. When he got it and saw what's in it, he'd say we'd better send that to the White House and the Attorney General so they can have in one place everything that the FBI has now on this guy. . . . (Bishop deposition, 12/2/75, pp. 141–142.)"

[75] None of these letters indicate that they were in response to requests, as is the case with other similar letters examined by the Committee. All were volunteered as matters which Director Hoover considered to be "of interest" to the recipients.

[76] Memorandum from Hoover to Vaughn, 2/15/47.

[77] Memorandum from Hoover to Connelly, 1/27/50.

[78] Memorandum from Hoover to Anderson, 4/21/55.

To Robert Cutler, Special Assistant to President Eisenhower, a report of a "confidential source" on plans of Mrs. Eleanor Roosevelt to hold a reception for the head of a civil rights group.[79]

To Attorney General Robert Kennedy, information from a Bureau "source" regarding plans of a group to publish allegations about the President's personal life.[80]

To Attorney General Kennedy, a summary of material in FBI files on a prominent entertainer which the FBI Director thought "may be of interest".[81]

To Marvin Watson, Special Assistant to President Johnson, a summary of data in Bureau files on the author of a play satirizing the President.[82]

As these illustrations indicate, the FBI Director provided such data to administrations of both political parties without apparent partisan favoritism.[83]

Additionally, during the Nixon Administration, the FBI's INLET (Intelligence Letter) Program for sending regular short summaries of FBI intelligence to the White House was used on one occasion to provide information on the purely personal relationship between an entertainer and the subject of an FBI domestic intelligence investigation.[84] SACs were instructed under the INLET program to submit to Bureau headquarters items with an "unusual twist" or regarding "prominent" persons.[85]

One reason for the Bureau's volunteering information to the White House was to please the Administration and thus presumably to build high-level political support for the FBI. Thus, a 1975 Bureau report on the Atlantic City episode states:

> One [agent said], "I would like to state that at no time did I ever consider (it) to be a political operation but it was obvious that DeLoach wanted to impress Jenkins and Moyers with the Bureau's ability to develop information which would be of interest to them." Furthermore, in response to a question as to whether the Bureau's services were being utilized for political reasons, [another] answered, "No. I do recall, however, that on one occasion I was present when DeLoach held a lengthy telephone conversation with Walter Jenkins. They appeared to be discussing the President's 'image.' At the end of the conversation DeLoach told us something to the effect, 'that may have sounded a little political to you but this doesn't do the Bureau any harm.' "[86]

In addition to providing information useful to superiors, the Bureau assembled information on its own critics and on political figures it believed might influence public attitudes or congressional support. FBI Director Hoover had massive amounts of information at his

[79] Memorandum from Hoover to Cutler, 2/13/58.
[80] Memorandum from Hoover to Robert Kennedy, 11/20/63.
[81] Memorandum from Hoover to Robert Kennedy, 2/10/61.
[82] Memorandum from Hoover to Watson, 1/9/67.
[83] For additional examples, See Section II, pp. 51-53.
[84] Staff memorandum: Review of INLET letters, 11/18/75.
[85] Memorandum from FBI Headquarters to all SAC's, 11/26/69.
[86] Memorandum from Bassett to Callahan, 1/29/75.

94-528 O - 78 - 20

fingertips. As indicated above, he could have the Bureau's files checked on anyone of interest to him. He personally received political information and "personal tidbits" from the special agents in charge of FBI field offices.[87] This information, both from the files and Hoover's personal sources, was available to discredit critics.

The following are examples of how the Bureau disseminated information to discredit its opponents:

> In 1949 the FBI provided Attorney General J. Howard McGrath and Presidential aide Harry Vaughn inside information on plans of the Lawyers Guild to denounce Bureau surveillance so they would have an opportunity to prepare a rebuttal well in advance of the expected criticism.[88]
>
> In 1960, when the Knoxville Area Human Relations Council in Tennessee charged that the FBI was practicing racial discrimination, the Bureau conducted name checks on members of the Council's board of directors and sent the results to Attorney General William Rogers, including derogatory personal allegations and political affiliations from as far back as the late thirties and early forties.[89]
>
> When a reporter wrote stories critical of the Bureau, he was not only refused any further interviews, but an FBI official in charge of press relations also spread derogatory personal information about him to other newsmen.[90]

The Bureau also maintained a "not to contact list" of "those individuals known to be hostile to the Bureau." Director Hoover specifically ordered that "each name" on the list "should be the subject of a memo." [91]

---

[87] Former FBI official Mark Felt has stated that the SAC's could have sent personal letters to Hoover containing such "personal tidbits" "to curry favor with him," and on one occasion he did so himself with respect to a "scandalous" incident. (W. Mark Felt testimony, 2/3/76, p. 91.)

The following excerpt from one SAC's letter is an example of political information fed to the Director: "I have heard several comments and items which I wanted to bring to your attention. As I imagine is true in all States at this time, the political situation in [this state] is getting to be very interesting. As you know, Senator [deleted] is coming up for re-election as is Representative [deleted]. For a long time it appeared that [the Senator] would have no opposition to amount to anything in his campaign for re-election. The speculation and word around the State right now is that probably [the Representative] will file for the U.S. Senate seat now held by [the Senator]. I have also been informed that [the Senator's] forces have offered [the Representative] $50,000 if he will stay out of the Senate race and run for re-election as Congressman." (Letter from SAC to Hoover, 5/20/64.)

[88] Letter from Attorney General McGrath to President Truman, 12/7/49; letter from Hoover to Vaughn, 1/14/50.

[89] Memorandum from Hoover to Rogers, 5/25/60.

[90] Bishop deposition, 12/2/75, p. 211. Bishop stated that he acted on his own, rather than at the direction of higher Bureau executives. However, Director Hoover did have a memorandum prepared on the reporter summarizing everything in the Bureau's files about him, which he referred to when he met with the reporter's superiors. (Bishop deposition, 12/2/75, p. 215.)

[91] Memorandum from Executives Conference to Hoover, 1/4/50. Early examples included historian Henry Steele Commager, "personnel of CBS," and former Interior Secretary Harold Ickes. (Memorandum from Mohr to Tolson, 12/21/49.) By the time it was abolished in 1972, the list included 332 names, including mystery writer Rex Stout, whose novel "The Doorbell Rang" had "presented a highly distorted and most unfavorable picture of the Bureau." (Memorandum from M. A. Jones to Bishop, 7/11/72.)

This request for "a memo" on each critic meant that, before someone was placed on the list, the Director received, in effect, a "name check" report summarizing "what we had in our files" on the individual.[92]

In addition to assembling information on critics, name checks were run as a matter of regular Bureau policy on all "newly elected Governors and Congressmen." The Crime Records Division instructed the field offices to submit "summary memoranda" on such officials, covering both "public source information" and "any other information that they had in their files." [93] These "summary memoranda" were provided to Director Hoover and maintained in the Crime Records Division for use in "congressional liaison"—which the Division head said included "selling" hostile Congressmen on "liking the FBI." [94]

It has been widely believed among Members of Congress that the Bureau had information on each of them.[95] The impact of that belief led Congressman Boggs to state:

> Our apathy in this Congress, our silence in this House, our very fear of speaking out in other forums has watered the roots and hastened the growth of a vine of tyranny which is ensnaring that Constitution and Bill of Rights which we are each sworn to uphold.
>
> Our society can survive many challenges and many threats. It cannot survive a planned and programmed fear of its own government bureaus and agencies.[96]

Subfinding (d)

The FBI has also used intelligence as a vehicle for covert efforts to influence social policy and political action.

The FBI's interference with the democratic process was not the result of any overt decision to reshape society in conformance with Bureau-approved norms. Rather, the Bureau's actions were the natural consequence of attitudes within the Bureau toward social change, combined with a strong sense of duty to protect society—even from its own "wrong" choices.

The FBI saw itself as the guardian of the public order, and believed that it had a responsibility to counter threats to that order, using any means available.[97] At the same time, the Bureau's assessment of what constituted a "threat" was influenced by its attitude toward the forces of change. In effect, the Bureau chose sides in the

---

[92] Bishop deposition, 12/2/75, p. 207.

[93] The field office was also expected to send to headquarters any additional allegations about the Congressman or Governor which might come to its attention in future investigations, even if the Congressman or Governor was not himself the "subject" of the investigation. (Bishop deposition, 12/2/75, pp. 194-200.)

[94] Bishop deposition, 12/2/75, pp. 206–7.

[95] The FBI is not the only agency believed to have files on Congressmen. According to Rep. Andrew Young, "in the freshman orientation" of new House members, "one of the things you are told is that there are seven agencies that keep files on private lives of Congressmen." (Rep. Andrew Young testimony, 2/19/76, p. 48.)

[96] Remarks by Rep. Hale Boggs, House of Representatives, 4/22/71, Congressional Record, Vol. 117, Part 9, p. 11562.

[97] The means used are discussed in the finding on "Covert Action to Disrupt and Discredit Domestic Groups", as well as the Detailed Reports on COINTELPRO, Dr. Martin Luther King, Jr., and the Black Panther Party.

major social movements of the last fifteen years, and then attacked the other side with the unchecked power at its disposal.

The clearest proof of the Bureau's attitude toward change is its own rhetoric. The language used in internal documents which were not intended to be disseminated outside the Bureau is that of the highly charged polemic revealing clear biases.

For example, in one of its annual internal reports on COINTELPRO, the Bureau took pride in having given "the lie" to what it called "the Communist canard" that "the Negro is downtrodden and has no opportunities in America." This was accomplished by placing a story in a newspaper in which a "wealthy Negro industrialist" stated that "the Negro will have to earn respectability and a responsible position in the community before he is accepted as an equal." It is significant that this view was expressed at about the same time as the civil rights movement's March on Washington, which was intended to focus public attention on the denial of opportunities to black Americans, and which rejected the view that inalienable rights have to be "earned." [98]

The rhetoric used in dealing with the Vietnam War and those in opposition to it is even more revealing. The war in Vietnam produced sharply divided opinions in the country; again, the Bureau knew which side it was on. For instance, fifty copies of an article entitled "Rabbi in Vietnam Says Withdrawal Not The Answer" were anonymously mailed by the FBI to members of the Vietnam Day Committee to "convince" the recipients "of the correctness of the U.S. foreign policy in Vietnam." [99]

The Bureau also ordered copies of a film called "While Brave Men Die" which depicted "communists, left-wing and pacifist activities associated with the so-called 'peace movement' or student agitational demonstrations in opposition to the United States position in Vietnam." The film was to be used for training Bureau personnel in connection with "increased responsibilities relating to communist inspired student agitational activities." [100]

In the same vein, a directive to the Chicago field office shortly after the 1968 Democratic Convention instructed it to "obtain all possible evidence" that would "disprove" charges that the Chicago police used undue force in dealing with antiwar demonstrations at the Convention:

> Once again, the liberal press and the bleeding hearts and the forces on the left are taking advantage of the situation in Chicago surrounding the Democratic National Convention to attack the police and organized law enforcement agencies. . . . We should be mindful of this situation and develop all possible evidence to expose this activity and to refute these false allegations.[101]

---

[98] Memorandum from FBI Headquarters to New York Field Office, et al., 8/13/63.

[99] Memorandum from FBI Headquarters to San Francisco Field Office, 11/11/65

[100] Memorandum from FBI Headquarters to New York Field Office et al., 3/9/66.

[101] Memorandum from FBI headquarters to Chicago Field Office 8/28/68.

The Bureau also attempted to enforce its view of sexual morality. For example, two students became COINTELPRO targets when they defended the use of a four-letter word, even though the demonstration in which they participated "does not appear to be inspired by the New Left," because it "shows obvious disregard for decency and established morality." [102] An anonymous letter purportedly from an irate parent and an article entitled "Free Love Comes to Austin" were mailed to a state senator and the chairman of the University of Texas Board of Regents to aid in "forcing the University to take action against those administrators who are permitting an atmosphere to build up on campus that will be a fertile field for the New Left." [103] And a field office was outraged at the distribution on campus of a newspaper called SCREW, which was described as "containing a type of filth that could only originate in a depraved mind. It is representative of the type of mentality that is following the New Left theory of immorality on certain college campuses." [104]

As these examples demonstrate, the FBI believed it had a duty to maintain the existing social and political order. Whether or not one agrees with the Bureau's views, it is profoundly disturbing that an agency of the government secretly attempted to impose its views on the American people.

(i) *Use of the Media*

The FBI attempted to influence public opinion by supplying information or articles to "confidential sources" in the news media. The FBI's Crime Records Division [105] was responsible for covert liaison with the media to advance two main domestic intelligence objectives: [106]

---

[102] Memorandum from FBI Headquarters to Minneapolis Field Office, 11/4/68.

[103] Memorandum from San Antonio field office to FBI Headquarters, 8/12/68; memorandum from FBI Headquarters to San Antonio Feld Office, 8/27/68.

[104] The field office also disapproved of the "hippy types" distributing the newspaper, with their "unkempt clothes", "wild beards", and "other examples of their nonconformity". Accordingly, an anonymous letter was sent to a state legislator protesting the distribution of such "depravity" at a state university, noting that "this is becoming a way of campus life. Poison the minds of the young, destroy their moral being, and in less than one generation this country will be ripe for its downfall." (Memorandum from New York Field Office to FBI Headquarters, 5/23/69; memorandum from FBI Headquarters to Newark Field Office, 1/69.

[105] The Crime Records Division also had responsibility for disseminating information to cultivate a favorable public image for the FBI—a practice common to many government agencies. This objective was pursued in various ways. One section of the Crime Records Division was assigned to assemble "material that was needed for a public relations program." This section "developed information for television shows, for writers, for authors, for newspapermen, people who wanted in-depth information concerning the FBI." The section also "handled scripts" for public service radio programs produced by FBI Field Offices; reviewed scripts for television and radio shows dealing with the FBI; and handled the "public relations and publicity aspect" of the "ten most wanted fugitives program." The Bureau attempted to assert control over media presentations of information about its activities. For example, Director Hoover's approval was necessary before the Crime Records Division would cooperate with an author intending to write a book about the FBI (Bishop testimony, 12/2/75, pp. 6–8, 18.)

[106] Memoranda recommending use of the media for COINTELPRO purposes sometimes bore the designation "Mass Media Program," which appeared merely to signify the function of the Crime Records Division as a "conduit" for disseminating information at the request of the Domestic Intelligence Division. (Bishop testimony, 12/2/75, pp. 63–68, 88.) The dissemination of derogatory information to the media was usually reviewed through the Bureau's chain of command and received final approval from Director Hoover. (Bishop testimony, 12/2/75, p. 89.)

(1) providing derogatory information to the media intended to generally discredit the activities or ideas of targeted groups or individuals; and (2) disseminating unfavorable articles, news releases, and background information in order to disrupt particular activities.

Typically, a local FBI agent would provide information to a "friendly news source" on the condition "that the Bureau's interest in these matters is to be kept in the strictest confidence." [107] Thomas E. Bishop, former Director of the Crime Records Division, testified that he kept a list of the Bureau's "press friends" in his desk.[108] Bishop and one of his predecessors indicated that the FBI sometimes refused to cooperate with reporters critical of the Bureau or its Director.[109]

Bishop stated that as a "general rule," the Bureau disseminated only "public record information" to its media contacts, but this category was viewed by the Bureau to include any information which could conceivably be obtained by close scrutiny of even the most obscure publications.[110] Within these parameters, background information supplied to reporters "in most cases [could] include everything" in the Bureau files on a targeted individual; the selection of information for publication would be left to the reporter's judgment.[111]

There are numerous examples of authorization for the preparation and dissemination of unfavorable information to discredit generally the activities and ideas of a target; [112]

—FBI headquarters solicited information from field offices "on a continuing basis" for "prompt . . . dissemination to the news media . . . to discredit the New Left movement and its adherents." Headquarters requested, among other things, that:

> specific data should be furnished depicting the scurrilous and depraved nature of many of the characters, activities, habits and living conditions representative of New Left adherents.

Field Offices were to be exhorted that "Every avenue of possible embarrassment must be vigorously and enthusiastically explored." [113]

—FBI headquarters authorized a Field Office to furnish a media contact with "background information and any arrest record" on a man

---

[107] For example, Memorandum from FBI Headquarters to Atlanta Field Office, 10/22/68.

[108] Bishop, 12/2/75, p. 33.

[109] Cartha DeLoach, who handled media contacts for several years, testified that this technique was not actually used as much as the Director desired:

> If any unfair comment appeared in any segment of the press concerning Mr. Hoover or the FBI . . . Mr. Hoover . . . would say do not contact this particular newspaper or do not contact this person or do not cooperate with this person. . . . If I had complied strictly to the letter of the law to Mr. Hoover's instructions, I think I would be fair in saying that we wouldn't be cooperating with hardly a single newspaper in the United States. . . . The men down through the years had to overlook some of those instructions and deal fairly with all segments of the press. (DeLoach testimony, 11/25/75, pp. 213–214.)

[110] Bishop stated that the Crime Records Division was "scrupulous" in providing information which could be cited to a "page and paragraph" in a public source. (Bishop, 12/2/75, pp. 24, 177–178.)

[111] Bishop, 12/2/75, pp. 135–136.

[112] T. E. Bishop stated that from the FBI documents available to the Committee, it was impossible to determine whether an article was actually printed after a news release or a draft article had been supplied to a media source. (Bishop, 12/2/75, p. 86.)

[113] Memorandum from C. D. Brennan to W. C. Sullivan, 5/22/68.

affiliated with "a radical New Left element" who had been "active in showing films on the Black Panthers and police in action at various universities during student rioting." The media contact had requested material from the Bureau which "would have a detrimental effect on [the target's] activities." [114]

—Photographs depicting a radical group's apartment as "a shambles with lewd, obscene and revolutionary slogans displayed on the walls" were furnished to a free-lance writer. The directive from headquarters said: "As this publicity will be derogatory in nature and might serve to neutralize the group, it is being approved." [115]

—The Boston Field Office was authorized to furnish "derogatory information about the Nation of Islam (NOI) to established source [name excised]":

> Your suggestions concerning material to furnish [name] are good. Emphasize to him that the NOI predilection for violence, preaching of race hatred, and hypocrisy, should be exposed. Material furnished [name] should be either public source or known to enough people as to protect your sources. Insure the Bureau's interest in this matter is completely protected by [name]. [116]

One Bureau-inspired documentary on the NOI reached an audience of 200,000. [117] Although the public was to be convinced that the NOI was "violent", the Bureau knew this was not in fact true of the organization as a whole. [118]

—The Section which supervised the COINTELPRO against the Communist Party intended to discredit a couple "identified with the Community Party movement" by preparing a news release on the drug arrest of their son, which was to be furnished to "news media contacts and sources on Capitol Hill." A Bureau official observed that the son's "arrest and the Party connections of himself and his parents presents an excellent opportunity for exploitation." The news release noted that "the Russian-born mother is currently under a deportation order" and had a former marriage to the son of a prominent Communist Party member. The release added: "the Red Chinese have long used narcotics to help weaken the youth of target countries." [119]

---

[114] Memorandum to Director from SAC Miami, 3/10/70. Bishop testified that he "would hope" that in response to the directive to disseminate the target's "arrest record" the Division would have disseminated only conviction records. Bishop said that under the Attorney General's guidelines then in effect only conviction records or arrests which were a matter of public record in a particular jurisdiction were to be disseminated. Bishop stated that his policy was not to disseminate an arrest record "especially if that arrest record resulted in an acquittal or if the charge was never completed . . . because that is not, to my mind, anything derogatory against a guy, until he actually gets convicted." (Bishop testimony, 12/2/75, pp. 163–167, 173.)

[115] Memorandum from FBI Headquarters to Boston Field Office, 1/13/68.

[116] Memorandum from FBI Headquarters to Boston Field Office, 2/27/68.

[117] Memorandum from Tampa Field Office to FBI Headquarters, 2/7/69.

[118] Deposition of Black Nationalist COINTELPRO supervisor, 10/17/75, p. 21; Deposition of George C. Moore, Chief of the Racial Intelligence Section, 11/3/75, p. 36.

[119] Memorandum from F. J. Baumgardner to W. C. Sullivan, 6/3/63.

—When the wife of a Communist Party leader purchased a new car, the FBI prepared a news item for distribution to "a cooperative news media source" mocking the leader's "prosperity" "as a disruptive tactic." The item commented sarcastically that "comrades of the self-proclaimed leader of the American working class should not allow this example of [the leader's] prosperity to discourage their continued contributions to Party coffers." [120]

—After a public meeting in New York City, where "the handling of the [JFK assassination] investigation was criticized," the FBI prepared a news item for placement "with a cooperative news media source" to discredit the meeting on the grounds that "a reliable [FBI] source" had reported a "convicted perjurer and identified espionage agent as present in the audience." [121]

—As part of the new Left COINTELPRO, the FBI sent a letter under a fictitious name to *Life* magazine to "call attention to the unsavory character" of the editor of an underground magazine, who was characterized as "one of the moving forces behind the Youth International Party, commonly known as the Yippies." To counteract a recent *Life* "article favorable" to the Yippie editor, the FBI's fictitious letter said that "the cuckoo editor of an unimportant smutty little rag" should be "left in the sewers." [122]

Much of the Bureau's use of the media to influence public opinion was directed at disrupting specific activities or plans of targeted groups or individuals:

—In March 1968, FBI Headquarters granted authority for furnishing to a "cooperative national news media source" an article "designed to curtail success of Martin Luther King's fund raising" for the poor people's march on Washington, D.C. by asserting that "an embarrassment of riches has befallen King . . . and King doesn't need the money." [123] To further this objective, Headquarters authorized the Miami Office "to furnish data concerning money wasted by the Poor People's Campaign" to a friendly news reporter on the usual condition that "the Bureau must not be revealed as the source." [124]

The Section Chief in charge of the Black Nationalist COINTELPRO also recommended that "photographs of demonstrators" at the march should be furnished; he attached six photographs of Poor People's Campaign participants at a Cleveland rally, accompanied by the note: "These show the militant, aggressive appearance of the participants and might be of interest to a cooperative news source." [125]

—As part of the New Left COINTELPRO, authority was granted to the Atlanta Field Office to furnish a newspaper editor who had "written numerous editorials praising the Bureau" with "information to supplement that already known to him from public sources concerning subversive influences in the Atlanta peace movement. His use of this material in well-timed articles would be used to thwart the [upcoming] demonstrations." [126]

[120] Memorandum from F. J. Baumardner to W. C. Sullivan, 8/9/65.
[121] Memorandum from F. J. Baumgardner to W. C. Sullivan, 2/24/64.
[122] Memorandum from New York Field Office to FBI Headquarters, 10/16/68.
[123] Memorandum from G. C. Moore to W. C. Sullivan, 10/26/68.
[124] Memorandum from FBI Headquarters to Miami Field Office, 7/9/68.
[125] Memorandum from G. C. Moore to W. C. Sullivan, 5/17/76.
[126] Memorandum from FBI Headquarters to Atlanta Field Office, 10/22/68.

—An FBI Special Agent in Chicago contacted a reporter for a major newspaper to arrange for the publication of an article which was expected to "greatly encourage factional antagonisms during the SDS Convention" by publicizing the attempt of "an underground communist organization" to take over SDS. This contact resulted in an article headlined "Red Unit Seeks SDS Rule." [127]

—FBI Director Hoover approved a Field Office plan "to get cooperative news media to cover closed meetings of Students for a Democratic Society (SDS) and other New Left groups" with the aim of "disrupting them." [128]

—Several months after COINTELPRO operations were supposed to have terminated, the FBI attempted to discredit attorney Leonard Boudin at the time of his defense of Daniel Ellsberg in the Pentagon Papers case. The FBI "called to the attention" of the Washington bureau chief of a major news service information on Boudin's alleged "sympathy" and "legal services" for "communist causes." The reporter placed a detailed news release on the wires which cited Boudin's "identification with Leftist causes" and included references to the arrest of Boudin's daughter, his legal representation of the Cuban government and "Communist sympathizer" Paul Robeson, and the statement that "his name also has been connected with a number of other alleged communist front groups." In a handwritten note, J. Edgar Hoover directed that copies of the news release be sent to "Haldeman, A. G., and Deputy." [129]

The Bureau sometimes used its media contacts to prevent or postpone the publication of articles it considered favorable to its targets of unfavorable to the FBI. For example, to influence articles which related to the FBI, the Bureau took advantage of a close relationship with a high official of a major national magazine, described in an FBI

[127] Memorandum from Chicago Field Office to FBI Headquarters, 6/18/69.

[128] Memorandum from FBI Headquarters to Indianapolis Field Office, 6/17/68.

[129] FBI Memorandum from Bishop to Mohr, 7/6/71; Bishop testimony, 12/2/75, pp. 148–151.

Two years earlier the Crime Records Division prepared a sixteen-page memorandum containing information on "Leonard B. Boudin, Attorney for Dr. Benjamin Spock," written at the time of Spock's indictment for conspiring to violate the Selective Service Act. (FBI Memorandum from M. A. Jones to T. E. Bishop, 2/26/68) The memorandum described "alleged associations and activities of Boudin" related to organizations or individuals considered "subversive" by the FBI. (Bishop, 12/2/75, pp. 134–135) and included: names of many of Boudin's clients; citations to magazines and journals in which Boudin had published articles; references to petitions he had signed; and notes on rallies and academic conferences at which he had spoken. The memorandum indicated that "the White House and Attorney General have been advised" of the information on Boudin's background. Notations on the cover sheet of the memorandum by high Bureau officials indicate that approval was granted for "furnishing the attached information to one of our friendly news contacts" but the information was not used until after the "results of appeal in Spock's case." Bishop did not recall distributing the Boudin memorandum. (Bishop, 12/2/75, pp. 125–126)

The head of the Crime Records Division speculated that the memorandum was prepared at the request of a reporter because he did not remember a request from Hoover or from the Domestic Intelligence Division, which was the normal route for assignments to the Crime Records Division. Division Chief Bishop testified that he probably instructed the Division "to get up any public source information that we have concerning Boudin that shows his connection with the Communist Party or related groups of that nature." (Bishop, 12/2/75, pp. 131–133)

memorandum as "our good friend." Through this relationship, the FBI "squelched" an "unfavorable article against the Bureau" written by a free-lance writer about an FBI investigation; "postponed publication" of an article on another FBI case; "forestalled publication" of an article by Dr. Martin Luther King, Jr.; and received information about proposed editing of King's articles.[130]

The Bureau also attempted to influence public opinion by using news media sources to discredit dissident groups by linking them to the Communist Party:

—A confidential source who published a "self-described conservative weekly newspaper" was anonymously mailed information on a church's sponsorship of efforts to abolish the House Committee on Un-American activities. This prompted an article entitled "Locals to Aid Red Line," naming the minister, among others, as a local sponsor of what it termed a "Communist dominated plot" to abolish HUAC.[131]

—The Bureau targeted a professor who had been the president of a local peace center, a "coalition of anti-Vietnam and anti-draft groups." In 1968, he resigned temporarily to become state chairman of Eugene McCarthy's presidential campaign organization. Information on the professor's wife, who had apparently associated with Communist Party members in the early 1950's, was furnished to a newspaper editor to "expose those people at this time when they are receiving considerable publicity in order" to "disrupt the members" of the peace organization.[132]

—Other instances included an attempt to link a school boycott with the Communists by alerting newsmen to the boycott leader's plans to attend a literary reception at the Soviet mission;[133] furnishing information to the media on the participation of the Communist Party presidential candidate in the United Farm Workers' picket line;[134] "confidentially" informing established sources in three northern California newspapers that the San Francisco County Communist Party Committee had stated that civil rights groups were to "begin working" on the area's large newspapers "in an effort to secure greater employment of Negroes;"[135] and furnishing information to the media on Socialist Workers Party participation in the Spring Mobilization Committee to End the War in Vietnam to "discredit" the antiwar group.[136]

(ii) Attacks on Leaders

Through covert propaganda, the FBI not only attempted to influence public opinion on matters of social policy, but also directly in-

[130] Memorandum from W. H. Stapleton to C. D. DeLoach, 11/5/64.

[131] Memorandum from Cleveland Field Office to FBI Headquarters, 10/28/64; memorandum from FBI Headquarters to Cleveland Field Office, 11/6/64.

[132] Memorandum from FBI Headquarters to Phoenix Field Office, 6/11/68.

[133] Memorandum from FBI Headquarters to New York Field Office, 2/4/64.

[134] The target was not intended to be the United Farm Workers, but a local college professor expected to participate in the picket line. The Bureau had unsuccessfully directed "considerable efforts to prevent hiring" the professor. Apparently, the Bureau did not consider the impact of this technique on the United Farm Workers' efforts. (Memorandum from San Francisco Field Office to FBI Headquarters, 9/12/68; memorandum from FBI Headquarters to San Francisco Field Office, 9/13/68.)

[135] Memorandum from San Francisco Field Office to FBI Headquarters, 4/16/64.

[136] Memorandum from San Francisco Field Office to FBI Headquarters, 3/10/67; memorandum from FBI Headquarters to San Francisco Field Office, 3/14/67.

tervened in the people's choice of leadership both through the electoral process and in other, less formal arenas.

For instance, the Bureau made plans to disrupt a possible "Peace Party" ticket in the 1968 elections. One field office noted that "effectively tabbing as communists or as communist-backed the more hysterical opponents of the President on the Vietnam question in the midst of the presidential campaign would be a real boon to Mr. Johnson." [137]

In the FBI's COINTELPRO programs, political candidates were targeted for disruption. The document which originated the Socialist Workers Party COINTELPRO noted that the SWP "has, over the past several years, been openly espousing its line on a local and national basis through running candidates for public office." The Bureau decided to "alert the public to the fact that the SWP is not just another socialist group but follows the revolutionary principles of Marx, Lenin, and Engels as interpreted by Leon Trotsky." Several SWP candidates were targeted, usually by leaking derogatory information about the candidate to the press.[138]

Other COINTELPRO programs also included attempts to disrupt campaigns. For example, a Midwest lawyer running for City Council was targeted because he and his firm had represented "subversives". The Bureau sent an anonymous letter to several community leaders which decried his "communist background" and labelled him a "charlatan." [139] Under a fictitious name, the Bureau sent a letter to a television station on which the candidate was to appear, enclosing a series of questions about his clients and his activities which it believed should be asked.[140] The candidate was defeated. He later ran (successfully, as it happened) for a judgeship. The Bureau attempted to disrupt this subsequent, successful campaign for a judgeship by using an anti-communist group to distribute fliers and write letters opposing his candidacy.[141]

In another instance, the FBI attempted to have a Democratic Party fundraising affair raided by the state Alcoholic Beverage Control Commission. The fund raiser was targeted because of two of the candidates who would be present. One, a state assemblyman running for reelection, was active in the Vietnam Day Committee; the other, the Democratic candidate for Congress, had been a sponsor of the National Committee to Abolish the House Committee on Un-American Activities and had led demonstrations opposing the manufacture of napalm bombs.[142]

Although the disruption of election campaigns is the clearest example, the FBI's interference with the political process was much broader.

[137] Memorandum from Chicago Field Office to FBI Headquarters, 6/1/67.
[138] Memorandum from FBI Headquarters to all SAC's, 10/12/61.
[139] Memorandum from Detroit Field Office to FBI Headquarters, 9/1/65; memorandum from FBI Headquarters to Detroit Field Office, 9/22/65.
[140] Memorandum from Detroit Field Office to FBI Headquarters, 9/28/65; memorandum from FBI Headquarters to Detroit Field Office, 10/1/65.
[141] Memorandum from Detroit Field Office, to FBI Headquarters, 1/19/67.
[142] Memorandum from FBI Headquarters to San Antonio Field Office, 11/14/66. The attempt was unsuccessful; a prior raid on a fire department's fund raiser had angered the local District Attorney, and the ABC decided not to raid the Democrats because of "political ramifications."

For example, all of the COINTELPRO programs were aimed at the leadership of dissident groups.[143]

In one case, the Bureau's plans to discredit a civil rights leader included an attempt to replace him with a candidate chosen by the Bureau. During 1964, the FBI began a massive program to discredit Dr. Martin Luther King, Jr. and to "neutralize" his effectiveness as the leader of the civil rights movement.[144] On January 8, 1964, Assistant Director William C. Sullivan proposed that the FBI select a new "national Negro leader" as Dr. King's successor after the Bureau had taken Dr. King "off his pedestal":

> When this is done, and it can and will be done . . . the Negroes will be left without a national leader of sufficiently compelling personality to steer them in the right direction. This is what could happen, but need not happen if the right kind of Negro leader could at this time be gradually developed so as to overshadow Dr. King and be in the position to assume the role of leadership of the Negro people when King has been completely discredited.
>
> I want to make it clear at once that I don't propose that the FBI in any way became involved openly as the sponsor of a Negro leader to overshadow Martin Luther King. . . . But I do propose that I be given permission to explore further this entire matter. . . .
>
> If this thing can be set up properly without the Bureau in any way becoming directly involved, I think it would not only be a great help to the FBI but would be a fine thing for the country at large. While I am not specifying at this moment, there are various ways in which the FBI could give this entire matter the proper direction and development. There are highly placed contacts of the FBI who might be very helpful to further such a step. . . .[145]

The Bureau's efforts to discredit Dr. King are discussed more fully elsewhere.[146] It is, however, important to note here that some of the Bureau's efforts coincided with Dr. King's activities and statements concerning major social and political issues.

(iii) Exaggerating The Threat

The Bureau also used its control over the information-gathering process to shape the views of government officials and the public on the

---

[143] The originating document for the "Black Nationalist" COINTELPRO ordered field offices to "expose, disrupt, misdirect, discredit, or otherwise neutralize" the "leadership" and "spokesmen" of the target groups. The "New Left" originating memo called for efforts to "neutralize" the New Left and the "Key Activitists," defined as "those individuals who are the moving forces behind the New Left;" the letter to field offices made it clear that the targets were the "leadership" of the "New Left"—a term which was never defined. (Memorandum from FBI Headquarters to all SAC's, 8/25/67.)

[144] Memorandum from Brennan to Sullivan, 5/9/68; memorandum from FBI Headquarters to all SAC's, 5/10/68.

[145] Memorandum from Sullivan to Belmont, 1/8/64. Although this proposal was approved by Director Hoover, there is no evidence that any steps were taken to implement the plan.

[146] See Martin Luther King, Jr. Report: Sec. V, The FBI's Efforts to Discredit Dr. Martin Luther King: 1964, Sec. VII, The FBI Program Against Dr. King: 1965–1968.

threats it perceived to the social order. For example, the FBI exaggerated the strength of the Communist Party and its influence over the civil rights and anti-Vietnam war movements.

Opponents of civil rights legislation in the early 1960s had charged that such legislation was "a part of the world Communist conspiracy to divide and conquer our country from within." The truth or falsity of these charges was a matter of concern to the administration, Congress, and the public. Since the Bureau was assigned to compile intelligence on Communist activity, its estimate was sought and, presumably, relied upon. Accordingly, in 1963, the Domestic Intelligence Division submitted a memorandum to Director Hoover detailing the CPUSA's "efforts" to exploit black Americans, which it concluded were an "obvious failure." [147]

Director Hoover was not pleased with this conclusion. He sent a sharp message back to the Division which, according to the Assistant Director in charge, made it "evident that we had to change our ways or we would all be out on the street." [148] Another memorandum was therefore written to give the Director "what Hoover wanted to hear." [149]

The memorandum stated, "The Director is correct;" it called Dr. Martin Luther King, Jr. "the most dangerous Negro of the future in this Nation from the standpoint of communism, the Negro, and national security;" and it concluded that it was "unrealistic" to "limit ourselves" to "legalistic proofs or definitely conclusive evidence" that the Communist Party wields "substantial influence over Negroes which one day could become decisive." [150]

Although the Division still had not said the influence *was* decisive, by 1964 the Director testified before the House Appropriations Subcommittee that the "Communist influence" in the "Negro movement" was "vitally important." [151] Only someone with access to the underlying information would note that the facts could be interpreted quite differently.[151a]

---

[147] Memorandum from Baumgardner to Sullivan, 8/23/63, p. 1.

[148] Sullivan deposition, 11/1/75, p. 20.

[149] Sullivan deposition, 11/1/75, p. 29.

[150] Memorandum from Sullivan to Director, FBI, 8/30/63. Sullivan described this process of "interpretive" memo writing to lead a reader to believe the Communists were influential without actually stating they were in control of a movement: "You have to spend years in the Bureau really to get the feel of this. . . . You came down here to 'efforts', these 'colossal efforts'. That was a key word of ours when we are getting around the facts. . . . You will not find anywhere in the memorandum whether the efforts were successful or unsuccessful. . . . Here is another one of our words that we used to cover up the facts, 'efforts to exploit', that word 'exploit'. Nowhere will you find in some of these memos the results of the exploitation. [Like] 'planning to do all possible', you can search in vain for a statement to the effect that their plans were successful or unsuccessful, partly successful or partly unsuccessful." (Sullivan, 11/1/75, pp. 15–16.)

[151] Hearings before the House Appropriations Subcommittee, 88th Cong., 2d Sess. (1964), p. 309. Director Hoover's statement was widely publicized. (E.g., "Hoover Says Reds Exploit Negroes," New York Times, 4/22/64, p. 30) It caused serious concern among civil rights leaders who feared that it would hurt the prospects for passage of the 1964 civil rights bill.

[151a] Director Hoover had included similar exaggerated statements about Communist influence in a briefing to the Eisenhower Cabinet in 1956. Hoover had stated, regarding an NAACP-sponsored conference:

"The Communist Party *plans* to use this conference to embarrass the Administration by causing a rift between the Administration and Dixiecrats who have

A similar exaggeration occurred in some of the Bureau's statements on communist influence on the anti-Vietnam war demonstrations.

In April 1965 President Johnson met with Director Hoover to discuss Johnson's "concern over the anti-Vietnam situation." According to Hoover, Johnson said he had "no doubt" that Communists were "behind the disturbances." [152] Hoover agreed, stating that upcoming demonstrations in eighty-five cities were being planned by the Students for a Democratic Society and that SDS was "largely infiltrated by communists and [it] has been woven into the civil rights situation which we know has large communist influence." [153]

Immediately after the meeting, however, Hoover told his associates that the Bureau might not be able to "technically state" that SDS was "an actual communist organization." The FBI merely knew that there were "communists in it." Hoover instructed, however, "What I want to get to the President is the background with emphasis upon the communist influence therein so that he will know exactly what the picture is." The Director added that he wanted "a good, strong memorandum" pinpointing that the demonstrations had been "largely participated in by communists even though they may not have initiated them;" the Bureau could "at least" say that they had "joined and forced the issue." According to the Director, President Johnson was "quite concerned" and wanted "prompt and quick action." [154]

Once again, the Bureau wrote a report which made Communist "efforts" sound like Communist success. The eight-page memorandum detailed all of the Communist Party's attempts to "encourage" domestic dissent by "a crescendo of criticism aimed at negating every effort of the United States to prevent Vietnam from being engulfed by communist aggressors." Twice in the eight pages, for a total of two and a half sentences, it was pointed out that most demonstrators were not Party members and their decisions were not initiated or controlled by the communists. Each of these brief statements moreover, was followed by a qualification: (1) "*however*, the Communist Party, USA . . . has vigorously supported these groups and exerted influence;" (2) "*While* the March [on Washington] was not Communist initiated . . . Communist Party members from throughout the nation participated." [Emphasis added.] [155]

The rest of the memorandum is an illustration of what former Assistant Director Sullivan called "interpretive" memo writing in

---

supported it, by forcing the Administration to take a stand on civil rights legislation with the present Congress. The Party *hopes* through a rift to affect the 1956 elections." [Emphasis added.] (Memorandum from Director, FBI, to the Executive Assistant to the Attorney General, 3/9/56, and enclosure.)

Director Hoover did not include in his prepared briefing statement the information reported to the White House separately earlier that there was "no indication" the the NAACP had "allowed the Communist Party to infiltrate the conference." (Hoover to Dillon Anderson, Special Assistant to the President, 3/5/56.) According to one historical account, Hoover's Cabinet briefing "reinforced the President's inclination to passivity" on civil rights legislation. (J. W. Anderson, *Eisenhower, Brownell, and the Congress: The Tangled Origins of the Civil Rights Bill of 1956-57* [University of Alabama Press, 1964], p. 34.)

[152] Memorandum from Hoover to subordinate FBI officials, 4/28/65.

[153] Hoover memorandum, 4/28/65.

[154] Hoover memorandum, 4/28/65.

[155] Letter from Hoover to McGeorge Bundy, Special Assistant to the President (National Security), 4/28/65, enclosing FBI memorandum, Subject: Communist Activities Relative to United States Policy on Vietnam.

which Communist efforts and desires are emphasized without any evaluation of whether they had been or were likely to be successful.

The exaggeration of Communist participation, both by the FBI and White House staff members relying on FBI reports,[156] could only have had the effect of reinforcing President Johnson's original tendency to discount dissent against the Vietnam War as "Communist inspired"—a belief shared by his successor.[157] It is impossible to measure the full effect of this distorted perception at the very highest policymaking level.

[156] See, *e.g.*, a memorandum from Marvin (Watson) to the President, 5/16/67, quoting from a Bureau report that: "the Communist Party and other organizations are continuing their efforts to force the United States to change its present policy toward Vietnam."

[157] The report prepared by the intelligence agencies as the basis for the 1970 "Huston Plan" included the following similar emphasis on the potential threat (and downplaying of the actual lack of success):

"Leaders of student protest groups" who traveled abroad were "considered to have *potential* for recruitment and participation in foreign-directed intelligence activity."

"Antiwar activists" who had "frequently traveled abroad" were considered "as having *potential* for engaging in foreign-directed intelligence collection."

The CIA was "of the view that the Soviet and bloc intelligence services *are committed* at the political level to exploit all domestic dissidents wherever possible."

Although there was "no hard evidence" of substantial foreign control of "the black extremist movement," there was "*a marked potential*" and the groups were "*highly susceptible* to exploitation by hostile foreign intelligence services."

"Communist intelligence services *are capable of* using their personnel, facilities, and agent personnel to work in the black extremist field."

While there were "no substantial indications that the communist intelligence services have actively fomented domestic unrest," their "*capability*" could not "*be minimized*."

"The dissidence and violence in the United States today present adversary intelligence services with *opportunities unparalleled* for forty years." [Emphasis added.] (Special Report, Interagency Committee on Intelligence (Ad Hoc), June 1970; substantial portions of this report appear in Hearings, Vol. 2, pp. 141-188.)