EXHIBIT A

TRANSCRIPT

May 15, 2007

COMMITTEE HEARING

SEN. PATRICK J. LEAHY
CHAIRMAN

SENATE JUDICIARY COMMITTEE
WASHINGTON, D.C.

SEN. PATRICK J. LEAHY HOLDS A HEARING ON THE U.S. ATTORNEY FIRINGS

CQ Transcriptions, LLC
1255 22nd Street N.W.
Washington, D.C. 20037
Transcript/Programming: Tel. 301-731-1728
Sales: Tel. 202-419-8500 ext 599
sales@cq.com
www.cq.com

the political needs of the president's party.

Before we get to the other issues, I want to go back to an incident from the time that Mr. Gonzales served as White House counsel.

There have been media reports describing a dramatic visit by Alberto Gonzales and Chief of Staff Andrew Card to the hospital bed of John Ashcroft in March 2004, after you, as acting attorney general, decided not to authorize a classified program.

First, can you confirm that a night-time hospital visit took place?

COMEY: Yes, I can.

SCHUMER: OK.

Can you remember the date and the day?

COMEY: Yes, sir, very well. It was Wednesday, March the 10th, 2004.

SCHUMER: And how do you remember that date so well?

COMEY: This was a very memorable period in my life; probably the most difficult time in my entire professional life. And that night was probably the most difficult night of my professional life. So it's not something I'd forget.

SCHUMER: Were you present when Alberto Gonzales visited Attorney General Ashcroft's bedside?

COMEY: Yes.

SCHUMER: And am I correct that the conduct of Mr. Gonzales and Mr. Card on that evening troubled you greatly?

COMEY: Yes.

SCHUMER: OK.

Let me go back and take it from the top.

You rushed to the hospital that evening. Why?

COMEY: I'm only hesitating because I need to explain why.

SCHUMER: Please. I'll give you all the time you need, sir.

COMEY: I've actually thought quite a bit over the last three years about how I would answer that question if it was ever asked, because I assumed that at some point I would have to testify about it.

The one thing I'm not going to do and be very, very careful about is, because this involved a classified program, I'm not going to get anywhere near classified information. I also am very leery of, and will not, reveal the content of advice I gave as a lawyer, the deliberations I engaged in. I think it's very important for the Department of Justice that someone who held my position not do that.

SCHUMER: In terms of privilege.

COMEY: Yes, sir.

SCHUMER: Understood.

COMEY: Subject to that, I -- and I'm uncomfortable talking about this...

SCHUMER: I understand.

COMEY: ... but I'll answer the question.

I -- to understand what happened that night, I, kind of, got to back up about a week.

SCHUMER: Please.

COMEY: In the early part of 2004, the Department of Justice was engaged -- the Office of Legal Counsel, under my supervision -- in a reevaluation both factually and legally of a particular classified program. And it was a program that was renewed on a regular basis, and required signature by the attorney general certifying to its legality.

And the -- and I remember the precise date. The program had to be renewed by March the 11th, which was a Thursday, of 2004. And we were engaged in a very intensive reevaluation of the matter.

And a week before that March 11th deadline, I had a private meeting with the attorney general for an hour, just the two of us, and

I laid out for him what we had learned and what our analysis was in this particular matter.

And at the end of that hour-long private session, he and I agreed on a course of action. And within hours he was stricken and taken very, very ill...

SCHUMER: (inaudible) You thought something was wrong with how it was being operated or administered or overseen.

COMEY: We had -- yes. We had concerns as to our ability to certify its legality, which was our obligation for the program to be renewed.

The attorney general was taken that very afternoon to George Washington Hospital, where he went into intensive care and remained there for over a week. And I became the acting attorney general.

And over the next week -- particularly the following week, on Tuesday -- we communicated to the relevant parties at the White House and elsewhere our decision that as acting attorney general I would not certify the program as to its legality and explained our reasoning in detail, which I will not go into here. Nor am I confirming it's any particular program.

That was Tuesday that we communicated that.

COMEY: The next day was Wednesday, March the 10th, the night of the hospital incident. And I was headed home at about 8 o'clock that evening, my security detail was driving me. And I remember exactly where I was -- on Constitution Avenue -- and got a call from Attorney General Ashcroft's chief of staff telling me that he had gotten a call...

SCHUMER: What's his name?

COMEY: David Ayers.

That he had gotten a call from Mrs. Ashcroft from the hospital. She had banned all visitors and all phone calls. So I hadn't seen him or talked to him because he was very ill.

And Mrs. Ashcroft reported that a call had come through, and that as a result of that call Mr. Card and Mr. Gonzales were on their way to the hospital to see Mr. Ashcroft.

SCHUMER: Do you have any idea who that call was from?

COMEY: I have some recollection that the call was from the president himself, but I don't know that for sure. It came from the White House. And it came through and the call was taken in the hospital.

So I hung up the phone, immediately called my chief of staff, told him to get as many of my people as possible to the hospital immediately. I hung up, called Director Mueller and -- with whom I'd been discussing this particular matter and had been a great help to me over that week -- and told him what was happening. He said, "I'll meet you at the hospital right now."

Told my security detail that I needed to get to George Washington Hospital immediately. They turned on the emergency equipment and drove very quickly to the hospital.

I got out of the car and ran up -- literally ran up the stairs with my security detail.

SCHUMER: What was your concern? You were in obviously a huge hurry.

COMEY: I was concerned that, given how ill I knew the attorney general was, that there might be an effort to ask him to overrule me when he was in no condition to do that.

SCHUMER: Right, OK.

COMEY: I was worried about him, frankly.

And so I raced to the hospital room, entered. And Mrs. Ashcroft was standing by the hospital bed, Mr. Ashcroft was lying down in the bed, the room was darkened. And I immediately began speaking to him, trying to orient him as to time and place, and try to see if he could focus on what was happening, and it wasn't clear to me that he could. He seemed pretty bad off.

SCHUMER: At that point it was you, Mrs. Ashcroft and the attorney general and maybe medical personnel in the room. No other Justice Department or government officials.

COMEY: Just the three of us at that point.

I tried to see if I could help him get oriented. As I said, it

wasn't clear that I had succeeded.

I went out in the hallway. Spoke to Director Mueller by phone. He was on his way. I handed the phone to the head of the security detail and Director Mueller instructed the FBI agents present not to allow me to be removed from the room under any circumstances. And I went back in the room.

I was shortly joined by the head of the Office of Legal Counsel assistant attorney general, Jack Goldsmith, and a senior staffer of mine who had worked on this matter, an associate deputy attorney general.

So the three of us Justice Department people went in the room. I sat down...

SCHUMER: Just give us the names of the two other people.

COMEY: Jack Goldsmith, who was the assistant attorney general, and Patrick Philbin, who was associate deputy attorney general.

I sat down in an armchair by the head of the attorney general's bed. The two other Justice Department people stood behind me. And Mrs. Ashcroft stood by the bed holding her husband's arm. And we waited.

And it was only a matter of minutes that the door opened and in walked Mr. Gonzales, carrying an envelope, and Mr. Card. They came over and stood by the bed. They greeted the attorney general very briefly. And then Mr. Gonzales began to discuss why they were there -- to seek his approval for a matter, and explained what the matter was -- which I will not do.

And Attorney General Ashcroft then stunned me. He lifted his head off the pillow and in very strong terms expressed his view of the matter, rich in both substance and fact, which stunned me -- drawn from the hour-long meeting we'd had a week earlier -- and in very strong terms expressed himself, and then laid his head back down on the pillow, seemed spent, and said to them, "But that doesn't matter, because I'm not the attorney general."

SCHUMER: But he expressed his reluctance or he would not sign the statement that they -- give the authorization that they had asked, is that right?

COMEY: Yes.

COMEY: Correct.

SPECTER: Well, how about what the president himself told you?

COMEY: I don't want to get into what -- the reason I hesitate, Senator Specter, is the right thing was done here, in part -- in large part because the president let somebody like me and Bob Mueller meet with him alone.

And if I talk about that meeting, I worry that the next president who encounters this is not going to let the next me get close to them to talk about something this important.

So I'm -- I want to be very careful that I don't talk about what the president and I talked about.

I met with the president. We had a full and frank discussion, very informed. He was very focused.

Then Director Mueller met with the president alone. I wasn't there.

Director Mueller carried to me the president's direction that we do what the Department of Justice wanted done to put this on a sound legal footing.

SPECTER: So you met first with the president alone for 15 minutes?

COMEY: Yes, sir.

SPECTER: And then Director Mueller met separately with the president for 15 minutes?

COMEY: I don't remember exactly how long it was. It was about the same length as my meeting. I went down and waited for him, as he...

SPECTER: And then Director Mueller, as you've testified, said to you, the president told Director Mueller to tell you to do what the Department of Justice thought was right?

COMEY: Correct.

SPECTER: Well -- but you won't say whether the president told you to do what the Department of Justice said was right?

COMEY: Yes, I...

SPECTER: You're not slicing hair. There's no hair there.

COMEY: You're a good examiner.

And that...

SPECTER: Well, thank you.

COMEY: Yes. I -- the president and I -- I don't think the conversation was finished. We discussed the matter in some detail. And then I urged him to talk to Bob Mueller about it.

And I don't know the content of Director Mueller's communication with him, except that Director Mueller -- the president didn't give me that -- I can answer that question.

The president didn't give me that direction at the end of our 15 minutes.

SPECTER: He did not?

COMEY: He did not. Instead, he said, "I'll talk to Director Mueller," as I had suggested.

Director Mueller came and met with him, then Director Mueller came to me and said that, "The president told me that the Department of Justice should get this where it wants to be, to do what the department thinks is right."

And I took that mandate and set about to do that, and accomplished that.

SPECTER: I thought you testified, in response to Senator Schumer's questions, that after meeting with the president for 15 minutes, he told you to do what you thought was right.

COMEY: If I did, I misspoke, because that direction came from the president to Director Mueller to me.

SPECTER: Well, when you had the discussions with Chief of Staff Card, what did he say to you by way of trying to pressure you, if, in fact, he did try to pressure you, to give the requisite certification?

SPECTER: Addington?

COMEY: Mr. Addington. The vice president told me that he disagreed. I don't remember any other White House officials telling me they disagreed.

SPECTER: OK. So you've got Card, Gonzales, Vice President Cheney and Addington who told you they disagreed with you.

COMEY: Yes, sir.

SPECTER: Did the vice president threaten you?

COMEY: No, sir.

SPECTER: Did Addington threaten you?

COMEY: No, sir.

SPECTER: So all these people told you they disagreed with you?

Well, why in this context, when they say they disagreed with you and you're standing by your judgment, would you consider resigning? You were acting attorney general. They could fire you if they wanted to. The president could replace you. But why consider resigning?

You had faced up to Card and Gonzales and Vice President Cheney and Addington, had a difference of opinion. You were the acting attorney general, and that was that. Why consider resigning?

COMEY: Not because of the way I was treated but because I didn't believe that as the chief law enforcement officer in the country I could stay when they had gone ahead and done something that I had said I could find no legal basis for.

SPECTER: When they said you could find no legal basis for?

COMEY: I had reached a conclusion that I could not certify as...

SPECTER: Well, all right, so you could not certify it, so you did not certify it.

But why resign? You're standing up to those men. You're not going to certify it. You're the acting attorney general. That's that.

COMEY: Well, a key fact is that they went ahead and did it without -- the program was reauthorized without my signature and without the Department of Justice. And so I believed that I couldn't stay...

SPECTER: Was the program reauthorized without the requisite certification by the attorney general or acting attorney general?

COMEY: Yes.

SPECTER: So it went forward illegally.

COMEY: Well, that's a complicated question. It went forward without certification from the Department of Justice as to its legality.

SPECTER: But the certification by the Department of Justice as to legality was indispensable as a matter of law for the program to go forward, correct?

COMEY: I believed so.

SPECTER: Then it was going forward illegally.

COMEY: Well, the only reason I hesitate is that I'm no presidential scholar.

But if a determination was made by the head of the executive branch that some conduct was appropriate, that determination -- and lawful -- that determination was binding upon me, even though I was the acting attorney general, as I understand the law.

And so, I either had to go along with that or leave. And I believed that I couldn't stay -- and I think others felt this way as well -- that given that something was going forward that we had said we could not certify as to its legality.

SPECTER: Well, I can understand why you would feel compelled to resign in that context, once there had been made a decision by the executive branch, presumably by the president or by the president, because he was personally involved in the conversations, that you would resign because something was going forward which was illegal.

The point that I'm trying to determine here is that it was going forward even though it was illegal.

COMEY: And I know I sound like I'm splitting hairs, but...

SPECTER: No, I don't think there's a hair there.

COMEY: Well, something was going forward without the Department of Justice's certification as to its legality. It's a very complicated matter, and I'm not going to go into what the program was or what the dimensions of the program...

SPECTER: Well, you don't have to.

If the certification by the Department of Justice as to legality is required as a matter of law, and that is not done, and the program goes forward, it's illegal. How can you -- how can you contest that, Mr. Comey?

COMEY: The reason I hesitate is I don't know that the Department of Justice's certification was required by statute -- in fact, it was not, as far as I know -- or by regulation, but that it was the practice in this particular program, when it was renewed, that the attorney general sign off as to its legality.

There was a signature line for that. And that was the signature line on which was adopted for me, as the acting attorney general, and that I would not sign.

So it wasn't going forward in violation of any -- so far as I know -- statutory requirement that I sign off. But it was going forward even though I had communicated, "I cannot approve this as to its legality."

And given that, I just -- I couldn't, in good conscience, stay.

SPECTER: Well, Mr. Comey, on a matter of this importance, didn't you feel it necessary to find out if there was a statute which required your certification or a regulation which required your certification or something more than just a custom?

COMEY: Yes, Senator. And I...

SPECTER: Did you make that determination?

COMEY: Yes, and I may have understated my knowledge. I'm quite certain that there wasn't a statute or regulation that required it, but that it was the way in which this matter had operated since the

beginning.

I don't -- I think the administration had sought the Department of Justice, the attorney general's certification as to form and legality, but that I didn't know, and still don't know, the source for that required in statute or regulation.

SPECTER: OK. Then it wasn't illegal.

COMEY: That's why I hesitated when you used the word "illegal."

SPECTER: Well, well, OK.

Now I want your legal judgment. You are not testifying that it was illegal. Now, as you've explained that there's no statute or regulation, but only a matter of custom, the conclusion is that even though it violated custom, it is not illegal.

It's not illegal to violate custom, is it?

COMEY: Not so far as I'm aware.

SPECTER: OK. So what the administration, executive branch of the president, did was not illegal.

COMEY: I'm not saying -- again, that's why I kept avoiding using that term. I had not reached a conclusion that it was.

The only conclusion I reached is that I could not, after a whole lot of hard work, find an adequate legal basis for the program.

SPECTER: OK.

Well, now I understand why you didn't say it was illegal. What I don't understand is why you now won't say it was legal.

COMEY: Well, I suppose there's an argument -- as I said, I'm not a presidential scholar -- that because the head of the executive branch determined that it was appropriate to do, that that meant for purposes of those in the executive branch it was legal.

I disagreed with that conclusion. Our legal analysis was that we couldn't find an adequate legal basis for aspects of this matter. And for that reason, I couldn't certify it to its legality.

SPECTER: OK.

FEINSTEIN: I'm not asking you to. I'm asking you, what piece of paper did you have to sign?

COMEY: It was a signature line on a presidential order.

FEINSTEIN: OK. All right.

And you said that the program was later changed so that it could be signed. But it went ahead at that time without your certification on it.

COMEY: Yes.

FEINSTEIN: And what was the elapsed period of time from that meeting, the denial of DOJ to certify the program and the time when it was essentially certified?

COMEY: It was reauthorized on Thursday, March the 11th, without the department's -- without my signature, without the department's approval.

And it was the next day -- so less than 24 hours later -- that we received the direction from the president to make it right.

And then we set about -- I don't remember exactly how long it was -- over the next few weeks making changes so that it accorded with our judgment about what could be certified as to legality.

And so it was really only that period from Thursday, when it was reauthorized, until I got the direction from the president the next day that it operated outside the Department of Justice's approval.

FEINSTEIN: For approximately two weeks?

COMEY: I don't remember exactly. It was two or three weeks I think that it took us to get the analysis done and make the changes that needed to be made.

FEINSTEIN: And then who signed for DOJ?

COMEY: It was either the attorney general, Ashcroft, or myself who signed. I may have signed that first one after the hospital incident.

FEINSTEIN: OK.

EXHIBIT B

Written Questions to
Former Deputy Attorney General James B. Comey
Submitted by Senator Patrick Leahy
May 22, 2007

1. You testified that the Department of Justice ("DoJ") completed a factual and legal evaluation of "a particular classified program" in 2004, and this review was conducted by, among others, the Office of Legal Counsel ("OLC").

a. When was this review started?

I believe some time in late fall 2003.

b. Why was the review started? Was the review started at the request of any individual or entity? If so, who or what entity**?**

I believe it was started at the initiative of Jack Goldsmith and Patrick Philbin.

c. Who participated in the review? Other than OLC, did any other division, section, or unit at DoJ participate in the review?

Goldsmith and Philbin were the principal participants, as I recall. I believe they were assisted from time to time by James Baker from the Office of Intelligence Policy and Review and my chief of staff, Chuck Rosenberg. There may have been other DOJ lawyers who assisted them.

d. Did any individual or entity from outside DoJ participate in the review? Were there any individuals from the White House, the Department of Defense ("DoD"), or other federal agency who participated in the review? If so please identify those individuals and/or entities?

I believe Goldsmith and Philbin coordinated their effort with lawyers in the intelligence community.

e. Did the review assess the full duration of the classified program and, if not, what time frame was reviewed?

The review focused on current operations during late 2003 and early 2004, and the legal basis for the program.

f. As a result of the review, did any individual or entity at DoJ, or any other agency, prepare a legal opinion or memorandum related to the classified program, and, if so, who or what entity prepared the legal opinion or memorandum?

OLC prepared legal memoranda concerning the matter, some of which would have been drafts. I also prepared at least one memorandum.

g. Were the results of this review shared with the Federal Bureau of Investigation ("FBI"), and, if so, who at the FBI and when?

It is my understanding that Goldsmith and Philbin discussed their work with officials from the General Counsel's office at the FBI, including the General Counsel, Valerie Caproni. I discussed the matter privately with FBI Director Mueller and FBI Deputy Director John Pistole.

h. Other than the White House or individuals at the White House, were the results of this review shared with any individual, entity, or federal agency outside DoJ, and, if so, who or what entity and when?

The matter was discussed with lawyers and non-lawyers in the intelligence community. I am uncomfortable going into more detail in an unclassified setting.

2. In your testimony, you stated that the views of DoJ related to the classified program were communicated to the White House prior to the evening of March 10, 2004.

a. How were these views communicated to the White House? Please identify whether the communications were made orally, in writing, by electronic communication, or other means; and to whom and when the communications were made. Please identify if any of the documents responsive to Question 1 above were included in this communication.

The views were communicated orally prior to March 10, 2004, including at a March 9 meeting I attended at the White House. I also believe that Goldsmith and Philbin had a variety of contacts with officials at the White House in the preceding weeks or months as the review was conducted. Those contacts may have involved their sharing written materials, but I am not sure. I recall sending one memorandum to the White House, after March 10, which I believe attached a memorandum written by Goldsmith.

b. Without disclosing the substance of the classified program or any legal advice, did these views include the understanding that the Attorney General, or you as Acting Attorney General, would not certify the classified program?

Yes.

c. Did you or others at DoJ receive any response to these views from the White House? If so, please identify whether the responses were made orally, in writing, by electronic communication, or other means; and to whom and when was the response was made.

I directly received oral responses during discussions at the White House on March 9, 2004. I know there were a variety of discussions in early 2004 in which I did not participate but that involved Jack Goldsmith and Patrick Philbin.

d. Did the response include any legal opinion or memorandum from the White House, or any other federal agency related to the classified program? If so, please identify what individual(s) or entities prepared and reviewed the legal opinion or memorandum.

I am not aware of any other such memorandum or legal opinion prior to March 10, 2004. Some time shortly after March 10, I received a memorandum from White House Counsel Gonzales.

3. You testified that after you arrived at the George Washington Hospital in Washington, D.C., on the evening of March 10, 2004, White House Counsel Alberto Gonzales and White House Chief of Staff Andrew Card came to Attorney General John Ashcroft's hospital room and spoke to him relating to the authorization of a classified program.

a. Did any individual(s) come with Mr. Gonzales or Mr. Card to the hospital, and if so, who? Were those individuals present for the conversation between Mr. Ashcroft and Mr. Gonzales?

I do not know with whom Mr. Gonzales and Mr. Card arrived; only the two of them entered the room.

b. Upon arriving in the hospital room, did Mr. Gonzales say anything to you, either before or after his conversation with Mr. Ashcroft, and if so, what did he say?

He did not speak to me at any time.

c. Did Mr. Card speak to Mr. Ashcroft or you in the hospital room and if so, what did he say?

Mr. Card did not speak to me. I believe he said, "Be well," to Attorney General Ashcroft as he turned to depart.

d. To your knowledge, did Mr. Gonzales or Mr. Card consult with Mr. Ashcroft's physician or any medical staff prior to entering the hospital room?

Not to my knowledge.

e. In your presence, did Mr. Gonzales or Mr. Card ask Mr. Ashcroft questions to elicit his state of mind and/or medical condition prior to discussing their request for authorization of the classified program?

I believe Mr. Gonzales began the conversation by asking, "How are you General?" to which the Attorney General replied, "Not well."

f. To your knowledge, did Mr. Gonzales or Mr. Card take any steps to ensure that facts related to the classified program were not disclosed to individuals without proper clearances or an actual need to know who were present in the hospital room?

Not to my knowledge.

4. In your testimony, you stated that FBI Director Robert Mueller also arrived at the George Washington Hospital that night.

a. To your knowledge, did Mr. Mueller have any conversation with Mr. Gonzales or Mr. Card at the hospital that night? If so, what was that conversation?

Not to my knowledge.

b. In your testimony, you indicated that Mr. Mueller had a "memorable" exchange with Mr. Ashcroft after Mr. Gonzales and Mr. Card left. Please describe that exchange.

It was a private conversation in which Mr. Mueller expressed his admiration for the Attorney General's conduct that evening.

5. You testified that the President met with you privately, and then, at your urging, he also met with Mr. Mueller privately, on the morning of March 12, 2004 following your daily counter-terrorism briefing. After these discussions, you stated that the President indicated to Mr. Mueller that you were now authorized to make changes to the classified program in response to the Department of Justice's views.

a. Following your meetings, did the President direct you or Mr. Mueller to discontinue or suspend any portion of classified program immediately until the appropriate changes were made to bring it into legal compliance?

No.

b. How long did the classified program continue without legal certification from DoJ?

I don't recall exactly, but believe it was approximately several weeks.

6. You testified that you discussed DoJ's views on the classified program with Vice President Dick Chaney and members of his staff, including his Chief of Staff David Addington.

a. Where and when did those discussions take place?

March 9, 2004 at the White House.

b. Who else was present for those discussions?

Jack Goldsmith, Patrick Philbin, Vice President Cheney, Mr. Addington, Mr. Card, Mr. Gonzales, and members of the intelligence community.

c. If those discussions were on or before March 10, 2004, was the Vice President and/or his staff aware of DoJ's decision not to certify the classified program? If so, how were they aware?

Yes. The Vice President was aware of DOJ's decision to not certify the program, because I had communicated this orally during a March 9 meeting. That meeting was a culmination of ongoing dialogue between DOJ and the White House.

d. If those discussions were on or before March 10, 2004, was the Vice President and/or his staff aware of your intention to resign if the classified program was authorized without DoJ certification? If so, how were they aware?

No. I had not made a decision to resign yet.

e. To your knowledge, did the Vice President or his staff have any role in the decision to have Mr. Card and Mr. Gonzales visit Mr. Ashcroft in the hospital? If so, what role did they have and what is the source for your information?

I have no knowledge about that.

7. You testified that Mr. Philbin, who was with you in the hospital, was "blocked from promotion," as a result of the position taken by DoJ related to this classified program.

a. Did any individual or individuals from the White House have any input into his potential promotion at DoJ? If so who, and in relation to what promotion?

Mr. Philbin was considered for principal Deputy Solicitor General after Paul Clement became Solicitor General. It was my understanding that the Vice President's office blocked that appointment.

b. Who was involved in blocking Mr. Philbin's promotion, and what did they do?

I understood that someone at the White House communicated to Attorney General Gonzales that the Vice President would oppose the appointment if the Attorney General pursued the matter. The Attorney General chose not to pursue it.

8. When did the Administration first conclude that the Authorization for Use of Military Force ("AUMF") authorized warrantless electronic surveillance of the type involved in what the Administration has called the "terrorism surveillance program" or TSP? If you do not recall a specific date, please provide as close an approximation as is possible.

I don't think it is appropriate for me to discuss legal advice by the Department of Justice or any particular classified program.

9. What legal standard for intercepting communications was the National Security Agency ("NSA") applying in its warrentless electronic surveillance program before March 2004? Was it a "probably cause" standard? What standard was the NSA applying when the program was first authorized? What standard was applied after March 2004?

I don't think it is appropriate for me to discuss legal advice by the Department of Justice or any particular classified program.

10. Has the warrantless electronic surveillance program always required before authorizing interception of a communication that at least one party to the communication be located outside of the United States? If not, approximately when did this become a requirement?

I don't think it is appropriate for me to discuss legal advice by the Department of Justice or any particular classified program.

11. Has the warrantless electronic surveillance program always required before authorizing interception of a communication that at least one party to the communication be a member or agent of Al Queda or an affiliate terrorist organization? If not, approximately when did this become a requirement?

I don't think it is appropriate for me to discuss legal advice by the Department of Justice or any particular classified program.

EXHIBIT C

HEARING OF THE HOUSE COMMITTEE ON THE JUDICIARY
SUBJECT: FBI OVERSIGHT
CHAIRED BY: REP. JOHN CONYERS
(D-MI)
WITNESS: ROBERT MUELLER,
DIRECTOR, FBI

2141 RAYBURN HOUSE OFFICE BUILDING, WASHINGTON, D.C.
1:34 P.M. EDT, THURSDAY, JULY 26, 2007

summary of why you feel that that's so important?

MR. MUELLER: Generally speaking, as I adverted to in my opening remarks, the digitization, the ability of persons to communicate in a variety of ways through digital networks, whether it be Skype, voice over IP, otherwise, the ability of persons to utilize communication capabilities across international lines has grown immensely over the years, and the statutory framework has not kept up with it. It goes without saying that, as was shown on September 11th, we face threats from overseas that we never thought we would face prior to that happening, because of the oceans on both sides of us, but with internationalization, we have to be astute and flexible in understanding that those who wish to do us harm from overseas can quickly cross borders with the click of a mouse or come into the country.

One of the things we absolutely need to do is, to the extent possible, understand that we have to use all of our resources on persons who are not U.S. citizens in foreign countries to obtain information with regard to their communications traffic. With a United States citizen in the United States, there should be a different mechanism. We all agree. The FISA modernization statute that we have sought from Congress will upgrade those capabilities and allow us to do in some sense that which we were able to do before technology, when we were using the old technology, but have been barred from using given the provisions of the FISA statute.

But we have to recognize that the division between information from outside the country -- the division of that information from outside the country to the information inside the country has to be broken down. There has to be integration. There has to be use of full capabilities, particularly when it comes to non-U.S. persons.

REP. GALLEGLY: Thank you, Mr. Director. I --

REP. CONYERS: Would the gentleman -- are you finished?

REP. GALLEGLY: I just want to make a 15-second summary. It's clear, I think, to most of us that in order to get to the core of organizations like al Qaeda, who have absolute modernized, technological telecommunications ability, is to penetrate through the network. And without this modernization, I would -- I think we all know that it's going to be very difficult to penetrate that outside network to get to the core.

I thank you very much. I thank the gentleman for letting me speak out of turn.

your agents were prepared to resign because of -- leading up to controversy?

MR. MUELLER: Again, I'm uncomfortable getting into conversations I had with individuals because I do believe that individuals are entitled to my unfettered thoughts --

REP. WATT: Can you confirm that you had some serious reservations about the warrantless wiretapping program that kind of led up to this?

MR. MUELLER: Yes.

REP. WATT: Okay.

I thank the chairman, and I yield back.

REP. CONYERS: Thank you.

Now, Howard Coble of -- (short pause) -- South Carolina? --

REP. HOWARD COBLE (R-NC): North.

REP. CONYERS: -- North Carolina, former chairman of the Patent and Copyright Committee, now the ranking member, is recognized.

REP. COBLE: Thank you, Mr. Chairman. Mr. Mueller, good to have you with us. Thank you for your years of public service.

I'm going to ask you a provincial question. Tobacco being prominent in my state, have there been recent arrests regarding the trafficking of counterfeit cigarettes by terrorist groups?

MR. MUELLER: I would have to check on the recency. There was one notable case from several years ago with Hezbollah in which I know cigarettes were being shipped from North Carolina to, if I'm not mistaken, it was Detroit, and there was substantial prosecution. I would have to check to determine whether any additional prosecution since then.

EXHIBIT D

HEARING OF THE SENATE SELECT COMMITTEE ON INTELLIGENCE
PROPOSED FISA MODERNIZATION LEGISLATION

WITNESSES:

MR. MIKE McCONNELL, DIRECTOR OF NATIONAL INTELLIGENCE;

LTG KEITH ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY;

MR. KENNETH WAINSTEIN, ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY, DEPARTMENT OF JUSTICE;

MR. BENJAMIN POWELL, GENERAL COUNSEL, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE;

MR. VITO POTENZA, GENERAL COUNSEL, NATIONAL SECURITY AGENCY

CHAIRED BY: SENATOR JOHN D. ROCKEFELLER IV (D-WV)

LOCATION: 106 DIRKSEN SENATE OFFICE BUILDING, WASHINGTON, D.C.

TIME: 2:30 P.M. EDT
DATE: TUESDAY, MAY 1, 2007

SEN. ROCKEFELLER: This hearing has begun, and I welcome all of our testifiers. And other members of the committee will be coming in. I know some of the caucuses just broke up.

The Select Committee on Intelligence meets today in open session, something we don't ought to do, to consider whether the scope and application regarding the Surveillance Act needs to changed to reflect the evolving needs for the timely collection of foreign intelligence. An extraordinarily complicated subject, this is. At the committee's request, the administration has undertaken a comprehensive review of the Foreign Intelligence Surveillance Act, commonly referred to as FISA. Out of this review, the administration proposed -- it believes would modernize the laws governing the way in which we gather foreign intelligence with the use of electronic surveillance.

Consideration of the administration's proposal and alternatives will be rooted in the Intelligence Committee's 30-year experience with our nation's long and delicate effort to strike that elusive right balance between effective intelligence collection for our national security and the constitutional rights and privacy interests of Americans.

The Intelligence Committee's existence came out of the work of the Church Committee and others in the mid-'70s to bring to light abuses in the electronic surveillance of Americans. One of the committee's first tasks was to work with the Senate Judiciary Committee and with the Ford and Carter administrations from 1976 to 1978 to enact the Foreign Intelligence Surveillance Act. As we take a fresh look at the current law, we will again be working with our colleagues in the Senate Judiciary Committee.

FISA involves both the judicial process on the one hand and the collection of intelligence. Our committee's contribution to this process

MR. MIKE McCONNELL: Good afternoon, Chairman Rockefeller, Vice Chairman Bond, members of the committee. Thank you for inviting us to come today to engage with the Congress on legislation that will modernize the Foreign Intelligence Surveillance Act, as you mentioned, FISA -- I'll refer to it as FISA from this point on -- which was passed in 1978.

In response to your guidance from last year on the need to revise FISA, the administration has worked for over the past year, with many of you and your staff experts, to craft the proposed legislative draft. It will help our intelligence professionals, if passed, protect the nation by preventing terrorist acts inside the United States. Since 1978, FISA has served as the foundation to conduct electronic surveillance of foreign powers or agents of foreign powers inside the United States. We are here today to share with you the criticality -- critical important role that FISA plays in protecting the nation's security, and how I believe the proposed legislation will improve that role, while continuing to protect the civil and the privacy rights of all Americans.

The proposed legislation to amend FISA has four key characteristics. First, it makes the statute technology-neutral. It seeks to bring FISA up to date with the changes in communications technology that have taken place since 1978. Second, it seeks to restore FISA to its original focus on protecting the privacy interests of persons inside the United States. Third, it enhances the government's authority to secure assistance by private entities, which is vital for the intelligence community to be successful. And fourth, it makes changes that will streamline FISA administrative processes so that the intelligence community can use FISA as a tool to gather foreign intelligence information more quickly and more effectively.

The four critical questions, four critical questions that we must address in collection against foreign powers or agents of foreign powers are the following. First, who is the target of the communications? Second, where is the target located? Third, how do we intercept the communications? And fourth, where do we intercept the communications? Where we intercept the communications has become a very important part of the determination that must be considered in updating FISA.

As the committee is aware, I've spent the majority of my professional life in or serving the intelligence community. In that capacity, I've been both a collector of information and a consumer of intelligence information. I had the honor of serving as the director of the National Security Agency from 1992 to 1996. In that position, I was fully aware of how FISA serves a critical function enabling the collection of foreign intelligence information.

In my first 10 weeks on the job as the new director of National Intelligence, I immediately can see the results of FISA-authorized collection activity. The threats faced by our nation, as I have previously testified to this committee, are very complex and there are very many. I cannot overstate how instrumental FISA has been in helping the intelligence community protect the nation from terrorist attacks since September 11th, 2001.

Some of the specifics that support my testimony, as has been mentioned, cannot be discussed in open session. This is because certain information about our capabilities could cause us to lose the capability if known to the terrorists. I look forward to elaborating further on aspects of the issues in a closed session that is scheduled to follow.

I can, however, make the following summary-level comment about the current FISA legislation. Since the law was drafted in a period preceding today's global information technology transformation and does not address today's global systems in today's terms, the intelligence community is significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States.

Let me repeat that for emphasis. We are significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States. We must make the requested changes to protect our citizens and the nation. In today's threat environment, the FISA legislation is not agile enough to handle the community's and the country's intelligence needs. Enacted nearly 30 years ago, it has not kept pace with 21st century developments in communications technology. As a result, FISA frequently requires judicial authorization to collect the communications of non-U.S. -- that is, foreign -- persons located outside the United States.

Let me repeat again for emphasis. As a result, today's FISA requires judicial authorization to collect communications of non-U.S. persons -- i.e., foreigners -- located outside the United States. This clogs the FISA process with matters that have little to do with protecting civil liberties or privacy of persons in the United States. Modernizing FISA would greatly improve that process and relieve the massive amounts of analytic resources currently being used to craft FISA applications.

FISA was enacted before cell phones, before e-mail and before the internet was a tool used by hundreds of millions of people worldwide every day.

There are two kinds of communications. It's important to just recapture the fact, two kinds of communications: wire and wireless. It's either on a wire -- could be a copper wire, a fiber wire -- it's on a wire or it's wireless, meaning it's transmitted through the atmosphere.

When the law was passed in 1978, almost all local calls were on a wire. Almost all local calls, meaning in the United States, were on a wire, and almost all long-haul communications were in the air, were known as wireless communications. Therefore, FISA in 1978 was written to distinguish between collection on a wire and collection out of the air or against wireless.

Now in the age of modern communications today, the situation is completely reversed. It's completely reversed. Most long-haul communications -- think overseas -- are on a wire -- think fiberoptic pipe. And local calls are in the air. Think of using your cell phone for mobile communications.

Communications technology has evolved in ways that have had unforeseen consequences under FISA, passed in 1978. Technological changes have brought within FISA's scope communications that we believe the 1978 Congress did not intend to be covered. In short, communications currently fall under FISA that were originally excluded from the act. And that is foreign-to-foreign communications by parties located overseas.

The solution is to make FISA technology-neutral. Just as the Congress in 1978 could not anticipate today's technology, we cannot know what technology may bring in the next thirty years. Our job is to make the country as safe as possible by providing the highest quality intelligence available. There is no reason to tie the nation's security to a snapshot of outdated technology.

Additionally, FISA places a premium on the location of the collection. Legislators in 1978 could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today, a single communication can transit the world even if the two people communicating are only located a few miles apart. And yet simply because our law has not kept pace with technology, communications intended to be excluded from FISA are in fact included. There is no real consequence -- this has real consequence on the intelligence community working to protect the nation.

Today intelligence agencies may apply, with the approval of the attorney general and the certification of other high level officials, for court orders to collect foreign intelligence information under FISA. Under the existing FISA statute, the intelligence community is often required to make a showing of probable cause.

Frequently, although not always, that person's communications are with another foreign person overseas. In such cases, the statutory requirement is to obtain a court order, based on a showing of probable cause, that slows, and in some cases prevents altogether, the government's effort to conduct surveillance of communications it believes are significant to national security, such as a terrorist coordinating attacks against the nation located overseas.

This is a point worth emphasizing, because I think many Americans would be surprised at what the current law requires. To state the case plainly: when seeking to monitor foreign persons suspected of involvement in terrorist activity who are physically located in foreign countries, the intelligence community is required under today's FISA to obtain a court order to conduct surveillance. We find ourselves in a position, because of the language in the 1978 FISA statute, simply -- we have not kept pace with the revolution in communications technology that allows the flexibility we need.

As stated earlier, this committee and the American people should know that the information we are seeking is foreign intelligence information. Specifically, this includes information relating to the capabilities, intentions and activities of foreign powers or agents of foreign powers, including information on international terrorist activities. FISA was intended to permit the surveillance of foreign intelligence targets while providing appropriate protection through court supervision to U.S. citizens and other persons located inside the United States.

Debates concerning the extent of the president's constitutional powers were heated in the mid-'70s, as indeed they are today. We believe that the judgment of the Congress at that time was that the FISA regime of court supervision was focused on situations where Fourth Amendment interests of persons in the United States were implicated. Nothing -- and I would repeat -- nothing in the proposed legislation changes this basic premise in the law.

complete understanding of how the statute has been interpreted and how it's being currently used. I don't know how you legislate that way. MR. WAINSTEIN: Well, I understand, but obviously, every time they issue an order, that is -- that can be an interpretation of how the FISA statute is -- interpretation of the FISA statute. And as you know from the numbers that we issue, we have a couple thousand FISAs a year. So that would be quite a few documents.

SEN. FEINGOLD: This is an important matter. If that's the number of items we need to look at, that's the number we will look at.

Thank you, Mr. Chairman.

SEN. ROCKEFELLER: Thank you, Senator Feingold.

Senator Nelson.

SEN. BILL NELSON (D-FL): Mr. Chairman, most of my questions I'm going to save for the closed session, but I would like to ascertain the administration's state of mind with regard to the current law. In the case where there is a foreign national in a foreign land calling into the United States, if you do not know the recipient's nationality and therefore it is possible it is a U.S. citizen, do you have to, in your interpretation of the current law, go and get a FISA order?

MR. McCONNELL: No, sir, not if it -- if the target is in a foreign country and our objective is to collect against the foreign target, and they call into the United States, currently it would not require a FISA. And let me double-check that. I may be -- I'm dated.

LTG ALEXANDER: If it's collected in the United States, it would require a FISA if we do not know who the end is to, or under the program it would have to be collected. If it were known, both ends foreign, known a priori, which is hard to do in this case, you would not. If it was collected overseas, you would not.

SEN. BILL NELSON: Let's go back to your second -- General, your second answer.

LTG ALEXANDER: If you know both ends -- where the call is going to go to before he makes the call, then you know that both ends were foreign; if you knew that ahead of time, you would not need a warrant.

SEN. NELSON: If you knew that.

LTG ALEXANDER: If you knew that.

SEN. NELSON: If you did not know that the recipient of the call in the U.S. is foreign, then you would have to have a FISA order.

LTG ALEXANDER: If you collected it in the United States. If you collected it overseas, you would not.

SEN. NELSON: Well, since in digital communications, if these things -- little packets of information are going all over the globe, you might be collecting it outside the United States, you might be collecting it inside the United States.

MR. McCONNELL: And Senator, that's our dilemma. In the time in 1978 when it was passed, almost everything in the United States was wire, and it was called electronic surveillance. Everything external in the United States was in the air, and it was called communications intelligence.

So what changed is now things in the United States are in the air, and things outside are on wire. That's the --

SEN. NELSON: I understand that, but -- now, I got two different answers to the same question from you, Mr. Director, and from you, General.

MR. McCONNELL: It depends on where the target is and where you collect it. That's why you heard different answers.

SEN. NELSON: So if you're collecting the information in the United States --

MR. McCONNELL: It requires a FISA.

SEN. NELSON: Okay. Under the current law, the president is allowed 72 hours in which he can go ahead and collect information and, after the fact, go back and get the FISA order.

Why was that suspended before in the collection of information?

LTG ALEXANDER: Sir, I think that would best be answered in closed session to give you exactly the correct answer, and I think I can do that.

SEN. NELSON: And -- well, then, you can acknowledge here that is -- it was in fact suspended.

SEN. ROCKEFELLER: I would hope that that would be -- we would leave this where it is.

SEN. NELSON: All right. I'll just stop there.

SEN. ROCKEFELLER: Thank you, Senator Nelson.

Senator Feinstein.

SEN. DIANNE FEINSTEIN (D-CA): Thank you very much, Mr. Chairman. The administration's proposal, Admiral, doesn't address the authority that the president and attorney general have claimed in conducting electronic surveillance outside of FISA. While the FISA Court issued a ruling that authorized the surveillance ongoing under the so-called TSP, Terrorist Surveillance Program, the White House has never acknowledged that it needs court approval. In fact, the president, under this reasoning, could restart the TSP tomorrow without court supervision if he so desired.

Now, Senator Specter and I have introduced legislation which very clearly establishes that FISA is the exclusive authority for conducting intelligence in the United States.

Here's the question: Does the administration still believe that it has the inherent authority to conduct electronic surveillance of the type done under the TSP without a warrant?

EXHIBIT E

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

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

JUNE 8, 1978.—Ordered to be printed

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

REPORT

together with

SUPPLEMENTAL, ADDITIONAL, AND DISSENTING VIEWS

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

The Permanent Select Committee on Intelligence, to whom was referred the bill (H.R. 7308) to amend title 18, United States Code, to authorize applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information, having considered the same, report favorably thereon with amendments and recommend that the bill as amended do pass.

AMENDMENTS

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

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

TABLE OF CONTENTS

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

II. STATEMENT OF NEED

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

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

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

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

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

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

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

III. SUMMARY OF LEGISLATION

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

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

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

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

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

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

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

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

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

IV. CONCLUSION

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

A basic premise behind this bill is the presumption that whenever an electronic surveillance for foreign intelligence purposes may in-

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Section 109

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

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

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

---

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

EXHIBIT F

LEGISLATIVE HISTORY
P.L. 95-511

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

P.L. 95-511, see page 92 Stat. 1783

Senate Report (Judiciary Committee) No. 95-604 (I and II), Nov. 15, 22, 1977 [To accompany S. 1566]

Senate Report (Intelligence Committee) No. 95-701, Mar. 14, 1978 [To accompany S. 1566]

House Report [Intelligence Committee) No. 95-1283, June 8, 1978 [To accompany H.R. 7308]

House Conference Report No. 95-1720, Oct. 5, 1978 [To accompany S. 1566]

Cong. Record Vol. 124 (1978)

DATES OF CONSIDERATION AND PASSAGE

Senate April 20, October 9, 1978

House September 7, October 12, 1978

The Senate bill was passed in lieu of the House bill. The Senate Reports (this page, p. 3970, p. 3973) and the House Conference Report (p. 4048) are set out.

SENATE REPORT NO. 95-604—PART 1

[page 1]

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

* * * * * * * * *

[page 3]

PURPOSE OF AMENDMENTS

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

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

balance to strike, but one which is necessary in our society, and a balance which cannot be achieved by sacrificing either our nation's security or our civil liberties. In my view this bill strikes the balance, sacrifices neither our security nor our civil liberties, and assures that the abuses of the past will remain in the past and that the dedicated and patriotic men and women who serve this country in intelligence positions, often under substantial hardships and even danger, will have the affirmation of Congress that their activities are proper and necessary.[1]

General Statement

I. Summary of the Legislation

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

[1] Hearing before the Subcommittee on Criminal Laws and Procedures of the Senate Committee on the Judiciary, Foreign Intelligence Surveillance Act of 1977, 95th Cong., 1st sess., p. 18 (1977) (hereinafter cited as "Senate Judiciary Hearings").

[page 5]

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

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

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

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

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

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

Under S. 1566, a judge may issue a warrant authorizing electronic surveillance within the United States only if he finds that: the President has authorized the Attorney General to approve applications for

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

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

[page 6]

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

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

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

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

In three major respects S. 1566 increases the protections for United States citizens and lawful resident aliens over those contained in S. 3197. First, the definition of electronic surveillance has been expanded to include the targeting of United States persons in their international communications. This is specifically aimed at eliminating one of the abuses identified by the Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities and largely implements one of that Committee's recommendations. (Book II, Intelligence Activities and the Rights of Americans, S. Rept. 94-755, 94th Cong., 2d Sess. 309 (1976).) Second, when a United States citizen

or lawful resident alien is the target of an electronic surveillance, the judge is required to review the Executive Branch certification to determine if it is clearly erroneous. No review of the certification was allowed in S. 3197. Finally, S. 1566 spells out that the Executive cannot engage in electronic surveillance within the United States without a prior judicial warrant. This is accomplished by repealing the so-called executive "inherent power" disclaimer clause currently found in section 2511(3) of Title 18, United States Code. S. 1566 provides instead that its statutory procedures (and those found in chapter 119 of title 18) "shall be the exclusive means" for conducting electronic surveillance, as defined in the legislation, in the United States. The highly controversial disclaimer has often been cited as evidence of a congressional ratification of the President's inherent constitutional power to engage in electronic surveillance in order to obtain foreign intelligence information essential to the national security. Despite the admonition of the Supreme Court that the language of the disclaimer was "neutral" and did not reflect any such congressional recognition of inherent power, the section has been a major source of controversy. By repeal-

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

II. STATEMENT OF NEED

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

The need for such statutory safeguards has become apparent in recent years. This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused. These abuses were initially illuminated in 1973 during the investigation of the Watergate break-in. Since that time, however, the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, chaired by Senator Church (hereafter referred to as the Church Committee), has concluded that every President since Franklin D. Roosevelt asserted the authority to authorize warrantless electronic surveillance, and exercised that authority. While the number of illegal or improper

national security taps and bugs conducted during the Nixon administration may have exceeded those in previous administrations, the surveillances were regrettably by no means atypical. In summarizing its

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

[2] See, e.g., Hearings before the Subcommittee on Criminal Laws and Procedures of the Senate Committee on the Judiciary, *Foreign Intelligence Surveillance Act of 1976*, 94th Cong., 2d sess. (1976); Senate Select Committee on Intelligence, *Foreign Intelligence Surveillance Act of 1978*, 94th Cong., 2d sess. (1978); Subcommittee on Surveillance of the Senate Committee on Foreign Relations and the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, *Warrantless Wiretaping and Electronic Surveillance*, 94th Cong., 1st sess. (1975); Joint Hearings before the Subcommittee on Administrative Practice and Procedure and the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, *Warrantless Wiretapping and Electronic Surveillance*, 93d Cong., 2d sess. (1974); Hearings before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, *Warrantless Wiretapping*, 92d Cong., 2d sess. (1972). In the joint report of the Subcommittees on Surveillance and Administrative Practice and Procedure issued in 1975, findings were made that "there are not adequate written standards or criteria within the executive branch to govern the warrantless electronic surveillance of either Americans or foreigners. There is a gap in the statutes, the case, and in administrative regulation on the use of warrantless wiretaps or bugs by executive branch agencies for alleged 'national security' purposes."

[page 8]

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

> Since the 1930's, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of judicial warrant. . . . [P]ast subjects of these surveillances have included a United States Congressman, Congressional staff member, journalists and newsmen, and numerous individuals and groups who engaged in no criminal activity and who posed no genuine threat to the national security, such as two White House domestic affairs advisers and an anti-Vietnam War protest group. (vol. 2, p. 12)
>
> * * * * *
>
> The application of vague and elastic standards for wiretapping and bugging has resulted in electronic surveillances which, by any objective measure, were improper and seriously infringed the Fourth Amendment Rights of both the targets and those with whom the targets communicated. The inherently intrusive nature of electronic surveillance, moreover, has enabled the Government to generate vast amounts of information—unrelated to any legitimate government interest—about the personal and political lives of American citizens. The collection of this type of information has, in turn, raised the danger of its use for partisan political and other improper ends by senior administration officials. (vol. 3, p. 32.)

Also formidable—although incalculable—is the "chilling effect" which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of the surveillance, but who perceived themselves, whether reasonably or unreasonably, as potential targets. Our Bill of Rights is concerned not only with direct infringements on constitutional rights, but also with government activities which effectively inhibit the exercise of these rights. The exercise of political freedom depends in large measure on citizens' understanding that they will be able to be publicly active and dissent

from official policy, within lawful limits, without having to sacrifice the expectation of privacy that they rightfully hold. Arbitrary or uncontrolled use of warrantless electronic surveillance can violate that understanding and impair that public confidence so necessary to an uninhibited political life.

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

> Electronic surveillance techniques have understandably enabled these agencies to obtain valuable information relevant to their legitimate intelligence missions. Use of these techniques has provided the Government with vital intelligence, which would be difficult to acquire through other means, about the activities and intentions of foreign powers and has
>
> [page 9]
>
> provided important leads in counterespionage cases. (vol. 2, p. 274)

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

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

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

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

III. BACKGROUND

The bipartisan congressional support for S. 1566 and the constructive cooperation of the Executive Branch toward the legislation signifies a constructive change in the ongoing debate over electronic sur-

veillance. That debate has centered around the power of the President to acquire information necessary for the national security and the constitutionality of warrantless electronic surveillance. This is not surprising since the United States Supreme Court has never expressly decided the issue of whether the President has constitutional authority to authorize warrantless electronic surveillance in cases concerning foreign intelligence. Whether the President has so-called "inherent power" to engage in or authorize warrantless electronic surveillance and, if such power exists, what limitations, if any, restrict the scope of that power, are issues which have troubled constitutional scholars for decades.

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

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

[4] 123 Cong. Rec. S7857 (daily ed., May 18, 1977).
[5] 277 U.S. 438, 48 S.Ct. 564, 72 L.Ed. 944.

[page 10]

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

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

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

This practice was continued in successive administrations. In 1946, Attorney General Tom C. Clark sent President Truman a letter informing him of President Roosevelt's directive. Clark's memorandum,

capable that Congress only intended to make clear that the Act simply did not legislate with respect to national security surveillances.

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

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

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

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

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

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

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

IV. Conclusion

S. 1566 would alter the current debate arising out of the uncertainty of the present law by completing an exclusive charter for the conduct

of electronic surveillance in the United States. It would relegate to the past the wire-tapping abuses brought to light during the committee hearings by providing, for the first time, effective substantive and procedural statutory controls over foreign intelligence electronic surveillance.[27]

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

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

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

2. 96 S.Ct. 1634, 48 L.Ed.2d 187. [page 16]

The basis for this legislation is the understanding—concurred in by the Attorney General—that even if the President has an "inherent" constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing foreign intelligence surveillance.[2]

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

One situation in which such a motion might be presented would be that in which the court orders disclosed to the party the court order and accompanying application under subsection (e) prior to ruling on the legality of the surveillance. Such motion would also be appropriate, however, even after the court's finding of legality if, in subsequent trial testimony, a Government witness provides evidence that the electronic surveillance may have been authorized or conducted in violation of the court order. The most common circumstance in which such a motion might be appropriate would be a situation in which a defendant queries the government under 18 U.S.C. 3504 and discovers that he has been intercepted by electronic surveillance even before the government has decided whether evidence derived from that surveillance will be used in the presentation of its case. In this instance, under the appropriate factual circumstances, the defendant might move to suppress such evidence under this subsection even without having seen any of the underlying documentation.

[55] 373 U.S. 83, 83 S.Ct. 1194, 10 L.Ed.2d 215 (1963).
[56] 18 U.S.C. 3500 et seq.
[57] *United States* v. *Andolschek*, 142 F. 2d 503 (2nd Cir. 1944).
[58] See also. *Alderman* v. *United States*, 394 U.S. 165 (1967).

[Page 57]

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

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

The special procedures in subsection (e) cannot be invoked until they are triggered by a Government affidavit that disclosure or an adversary hearing would harm the national security of the United States. If no such assertion is made, the Committee envisions that mandatory disclosure of the application and order, and discretionary disclosure of other surveillance materials, would be made to the defendant, as is required under Title III.[59] When the procedure is so triggered, however, the Government must make available to the court

a copy of the court order and accompanying application upon which the surveillance was based.

The court must then conduct an *ex parte*, *in camera* inspection of these materials as well as any other documents which the Government may be ordered to provide, to determine whether the surveillance was authorized and conducted in a manner which did not violate any constitutional or statutory right of the person against whom the evidence is sought to be introduced. The subsection further provides that in making such a determination, the court may order disclosed to the person against whom the evidence is to be introduced the court order or accompanying application, or portions thereof, or other materials relating to the surveillance, only if it finds that such disclosure is necessary to make an accurate determination of the legality of the surveillance. Thus, this subsection deals with the procedure to be followed by the trial court in determining the legality (or illegality) of the surveillance.

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

[8] 18 U.S.C. 2518 (9) and (10).

decided by the Supreme Court. As Justice Stewart noted in his concurring opinion in *Giordano* v. *United States*, "Moreover, we did not in *Alderman*, *Butenko* or *Ivanov*, and we do not today, specify the procedure that the District Courts are to follow in making this preliminary determination [of legality.]" 394 U.S. 310, 314 (1968); see also, *Taglianetti* v. *United States*, 394 U.S. 316 (1968)[8]. The committee views the procedures set forth in this subsection as striking a reasonable balance between an entirely *in camera* proceeding which might adversely affect the defendant's ability to defend himself, and mandatory disclosure, which might occasionally result in the wholesale revelation of sensitive foreign intelligence information.

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

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

Thus, in some cases, the court will likely be able to determine the legality of the surveillance without any disclosure to the defendant.

EXHIBIT G

question of how many "outouts" are enough to exempt an American acting on behalf of or in conjunction with a Communist regime from lawful electronic surveillance? Most Americans would probably agree that in such cases it would be better to err on the side of caution and tell the intelligence agencies to survey anyone working with such regimes. The bill ought to reflect this.

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

MALCOLM WALLOP.

HOUSE CONFERENCE REPORT NO. 95-1720

* * * * * * * * *

[page 19]

JOINT EXPLANATORY STATEMENT OF THE COMMITTEE OF CONFERENCE

The managers on the part of the House and the Senate at the conference on the disagreeing votes of the two Houses on the amendments of the House to the bill (S. 1566) to amend title 18, United States Code, to authorize applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information, submit the explanation of the effect of the action agreed upon by the managers and recommended in the accompanying conference report.

The managers recommend that the Senate agree to the amendments of the House, with an amendment. That amendment will be referred to here as the "conference substitute." Except for certain clarifying, clerical, conforming, and other technical changes, there follows an issue by issue summary of the Senate bill, the House amendments, and the conference substitute.

TITLE

The Senate bill amended Title 18 (Crimes and Criminal Procedures) of the United States Code, to authorize applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information.

The House amendments provided for an uncodified title, to authorize electronic surveillance to obtain foreign intelligence information.

The conference substitute adopts the House provision. The conferees agree that this change is not intended to affect in any way the jurisdiction of Congressional Committees with respect to electronic surveillance for foreign intelligence purposes. Rather, the purpose of the change is solely to allow the placement of Title I of the Foreign Intelligence Surveillance Act in that portion of the United States Code (Title 50) which most directly relates to its subject matter.

DEFINITION OF "FOREIGN POWER"

The Senate bill defined "foreign power", with respect to terrorist groups, to mean a foreign-based terrorist group.

[redacted]

NOTICE OF USE OF INFORMATION IN LEGAL PROCEEDINGS

The Senate bill provided for notification to the court when information derived from electronic surveillance is to be used in legal proceedings.

The House amendments contained a comparable provision and also a provision, not contained in the Senate bill, requiring notice to the aggrieved person. The House amendments also contained a separate section relating to use by State or local authorities requiring notice to the Attorney General.

The conference substitute adopts the House provisions. The conferees agree that notice should be given to the aggrieved person as soon as possible, so as to allow for the disposition of any motions concerning evidence derived from electronic surveillance. The conferees also agree that the Attorney General should at all times be able to assess whether and to what extent the use of information made available by the Government to a State or local authority will be used.

SUPPRESSION MOTIONS

The Senate bill provided for motions to suppress the contents of any communication acquired by electronic surveillance, or evidence derived therefrom.

The House amendments provided for motions to suppress the evidence obtained or derived from electronic surveillance.

The conference substitute adopts the House provision. The conferees agree that the broader term "evidence" should be used because it includes both the contents of communications and other information obtained or derived from electronic surveillance.

IN CAMERA PROCEDURE FOR DETERMINING LEGALITY

The Senate bill provided a single procedure for determining the legality of electronic surveillance in a subsequent in camera and ex parte proceeding, if the Government by affidavit asserts that disclosure or an adversary hearing would harm the national security of the United States. The Senate bill also provided that, in making this determination, the court should disclose to the aggrieved person materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

The House amendments provided two separate procedures for determining the legality of electronic surveillance, if the Attorney General files an affidavit under oath that disclosure would harm the national security of the United States or compromise foreign intelligence sources and methods. In criminal cases, there would be an in camera proceeding; and the court might disclose to the aggrieved person, under appropriate security procedures and protective orders, materials relating to the surveillance if there were a reasonable question as to the legality of the suveillance and if disclosure would likely promote a more accurate determination of such legality, or if disclosure would not harm the national security. In civil suits, there would be an in camera and ex parte proceeding before a court of appeals; and the court would disclose, under appropriate security procedures and protective orders, to the aggrieved person or his attorney materials relat-

ing to the surveillance only if necessary to afford due process to the aggrieved person. The House amendments also provided that orders regarding legality or disclosure would be final and binding.

The conference substitute essentially adopts the Senate provisions, with technical changes and the following modifications. The in camera and ex parte proceeding is invoked if the Attorney General files an affidavit under oath. All orders regarding legality and disclosure shall be final and binding only where the rulings are against the Government.

The conference substitute adds the words "requiring review or" to the provision making orders final and binding. This change clarifies the intent of the House provision in conformity with section 102(a). The conferees intend that a determination by a district court that review of a certification by the Attorney General under section 102(a) is necessary to determine the legality of the surveillance shall be considered a final and binding order and thus appealable by the Government before the court reviews the certification. The court may order that the certification be unsealed for review if such review is necessary to determine the legality of the surveillance.

The conferees agree that an in camera and ex parte proceeding is appropriate for determining the lawfulness of electronic surveillance in both criminal and civil cases. The conferees also agree that the standard for disclosure in the Senate bill adequately protects the rights of the aggrieved person, and that the provision for security measures and protective orders ensures adequate protection of national security interests.

UNINTENTIONAL RADIO ACQUISITION

The Senate bill prohibited any use of the contents of unintentionally acquired domestic radio communications, if there is a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, except where the contents indicate a threat of death or serious bodily harm to any person.

The House amendments contained a comparable provision, with an exception if the contents may indicate a threat of death or serious bodily harm to any person.

The conference substitute adopts the Senate provision which omits the word "may." The conferees agree that an exception for any indication of such a threat is sufficient.

CONGRESSIONAL OVERSIGHT

The Senate bill and the House amendments both require the Attorney General, on a semiannual basis, to fully inform the intelligence committees of each House concerning all electronic surveillance under the act.

The Senate bill also stated that "nothing in this chapter shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties."

The House amendments limited this reservation to the respective intelligence committees. The conference substitute adopts the Senate version.

Section 2528(b) of the Senate bill required the Senate Intelligence Committee to report annually to the Senate on the implementation of

vided for notice to the Attorney General or other appropriate official when or if any person who is ordered to provide assistance to the Government in conducting electronic surveillance is required by legal process to disclose the fact of such assistance. It also afforded civil immunity to any person who provides such assistance in accordance with a court order or Attorney General certificate.

The conference substitute adopts the House provisions, with the addition of the Senate provision imposing civil liability upon a common carrier which provides assistance without a court order or Attorney General certificate. Deletion of certain conforming amendments is consistent with the decision of the conferees not to place the bill in title 18, United States Code.

EXCLUSIVE MEANS FOR ELECTRONIC SURVEILLANCE

The Senate bill provided that the procedures in this bill and in chapter 119 of title 18, United States Code, shall be the exclusive means by which electronic surveillance, as defined in this bill, and the interception of domestic wire and oral communications may be conducted.

The House amendments provided that the procedures in this bill and in chapter 119 of title 18, United States Code, shall be the exclusive statutory means by which electronic surveillance as defined in this bill and the interception of domestic wire and oral communications may be conducted.

The conference substitute adopts the Senate provision which omits the word "statutory." The conferees agree that the establishment by this act of exclusive means by which the President may conduct electronic surveillance does not foreclose a different decision by the Supreme Court. The intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in the Steel Seizure Case: "When a President takes measures incompatible with the express or implied will of Congress, his power is at the lowest ebb, for then he can rely only upon his own Constitutional power minus any Constitutional power of Congress over the matter." *Youngstown Sheet and Tube Co.* v. *Sawyer*, 343 U.S. 579, 637 (1952)[1].

EDWARD P. BOLAND,
MORGAN F. MURPHY,
R. L. MAZZOLI,
PETER W. RODINO,
ROBERT W. KASTENMEIER,
Managers on the Part of the House.

EDWARD M. KENNEDY,
JAMES ABOUREZK,
HOWARD M. METZENBAUM,
BIRCH BAYH,
JOE BIDEN,
ROBERT MORGAN,
BILL HATHAWAY,
STROM THURMOND,
JAKE GARN,
CHARLES McC. MATHIAS, JR.,
Managers on the Part of the Senate.

1. 72 S.Ct. 863, 96 L.Ed. 1153.

EXHIBIT H

guise that he is an agent of a refugee terrorist leader and then to target these recruited persons against the FBI, the Dade County Police, and the CIA, the ultimate goal being to infiltrate these agencies. F is to keep the intelligence officer informed as to his progress in this regard but his reports are to be made by mail, because the U.S. Government cannot open the mail unless a crime is being committed.

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

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

SENATE REPORT NO. 95-701

[page 1]

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

* * * * * * * * *

[page 5]

PURPOSE OF AMENDMENTS

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

[redacted]

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

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

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

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

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

section further provides that in making such a determination, the court may order disclosed to the person against whom the evidence is to be introduced the court order or accompanying application, or portions thereof, or other materials relating to the surveillance, only if it finds that such disclosure is necessary to make an accurate determination of the legality of the surveillance.

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

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

394 U.S. 310, 314 (1968); see also, *Taglianetti* v. *United States*, 394 U.S. 316 (1968)[4]. The committee views the procedures set forth in this subsection as striking a reasonable balance between an entirely in camera proceeding which might adversely affect the defendant's ability to defend himself, and mandatory disclosure, which might occasionally result in the wholesale revelation of sensitive foreign intelligence information.

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

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

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

4. 89 S.Ct. 1099, 22 L.Ed.2d 302.

[33] Cf. *Alderman* v. *United States*, 394 U.S. 165, 182 n. 14, 89 S.Ct. 961, 22 L.Ed.2d 176 (1968); *Taglianetti* v. *United States*, supra at 317.