traditional procedures that it must adhere to; but when the same agency deals with the counterintelligence, national security, it is living in a different world. Would it be sensible to break the Bureau in two so that the part that deals with traditional law enforcement is that, and that alone, and that another department within the Justice Department and under the Attorney General would deal exclusively with national security and counterintelligence matters, that are really quite a different character than normal law enforcement?

Attorney General LEVI. Obviously, that is not a question that one answers without a great deal of thought. My own present view is that it would not be a good idea, because the point is to develop procedures which are adhered to just as vigorously in both areas. This is one reason we do have a committee which has been hard at work fashioning guidelines. These guidelines, when completed—I think the committee has seen some of them—will be in statutory or Executive order form.

But I think, whatever the shortcomings may have been in the past, that a strong attribute of the Bureau is its discipline, and that one wants to develop in this area—where, by the way, it is wrong in some sense to fault agencies when the law changed as it did. It would be desirable to develop procedures in that area which would evoke the same discipline and, although the area is quite different, there are comparable points, the checking, the reviewing, the getting permission, and so on. It is really a different world. One of the problems, Mr. Chairman, if I may say so, is when one looks at the past, one finds some terribly interesting things, but sometimes one forgets what the present is like.

The CHAIRMAN. I will not belabor the point, except to say when one agency does both kinds of work, I think that there is some danger, although it may be well-disciplined, for the methods in the one area to creep into the other. It may be more sensible to let counterintelligence and national security matters of that kind be handled by a separate bureau under the Justice Department. I would not want to see it all thrown into the CIA, for example; I want them to look outward in dealing with foreign countries, and not dealing with this country. But a separate department within Justice that deals with this quite separate matter from ordinary law enforcement, is an idea which I think should be given more thought.

Thank you very much for your testimony.

Our next witness is Prof. Philip Heymann of the Harvard Law School.

[The prepared statement of Prof. Philip Heymann in full follows:]

PREPARED STATEMENT OF PHILIP B. HEYMANN, PROFESSOR OF LAW, HARVARD LAW SCHOOL

I. INTRODUCTION

A. This Committee has heard evidence about a number of activities of the intelligence agencies which raise significant questions.

1. Two forms of activities are familiar:

a. Surreptitious entries.

b. Domestic electronic surveillance.

2. Two other forms of activity were previously unknown and raise comparatively novel questions:

a. The opening of mail to and from the United States.

b. The interception of cable and phone communications between the United States and foreign countries.

B. These activities and others the Committee has reviewed raise three sets of questions. I shall address only the last of the three, not because the others are unimportant or even less important but because time does not allow dealing with all of them on a single occasion.

1. There is a serious question about the collection of files on dissenters. I think there can be no serious doubt that an operation such as the "CHAOS" operation of the CIA tends to discourage participation in legitimate political activities, particularly by those who are somewhat timid. The Army intelligence gathering program raised similar questions.

2. Wholly separate from the question of the chilling effect of an excessive collection and maintenance of files, there are the unique problems that are created when intelligence agencies such as the CIA and NSA wander into the domestic area. These agencies are unlike our domestic investigative agencies in a number of relevant ways.

a. They are funded in the billions of dollars.

b. Their employees are trained to operate in secret circumstances abroad and without necessary conformity with local law.

c. The importance of secrecy makes the monitoring function performed for domestic agencies by the Congress, the courts, and the public at large much less applicable.

These characteristics led the Congress to attach a statutory prohibition to domestic activities of the CIA. I am aware that members of the Committee pressed General Allen on whether this would not also be desirable for the NSA.

3. The third subject for the Committee's concern, and the only one I intend to address today, is the problem of invading the privacy of communications of American citizens. This is an area that the Fourth Amendment of the Constitution and a number of statutes protect. In discussing this area I will attempt to make clear where the law is moderately firm and where it is uncertain. I shall also do my best to separate off my recommendations from my estimates of what the law is.

C. As we proceed to discuss these questions, it will become apparent that additional legislation would be highly desirable for several reasons.

1. We are dealing with the area of foreign policy and most particularly with the special situation of intelligence gathering and secret technology. This Committee and through it, the Congress, have a factual basis for assessing these matters which courts cannot duplicate. This is especially true after the Committee's extended set of hearings.

2. There are obvious and important gaps in the present law which legislation will be needed to fill. I will allude to these as I proceed.

II. THE EFFECT OF A GOVERNMENTAL INTEREST IN FOREIGN INTELLIGENCE ON THE FOURTH AMENDMENT RIGHTS OF CITIZENS

A. One question runs through each of the areas the Committee has been investigating: to what extent does the Fourth Amendment apply to matters of national security?

1. There are a series of additional difficulties to be addressed in connection with searches of international mail and international voice and non-voice communications.

2. But the same question as to what difference is made by a foreign intelligence objective applies to those programs as well as to more familiar searches of homes, offices, or domestic communications.

B. The Fourth Amendment provides two different forms of protection, each of which could be affected by the fact that the government is pursuing a foreign intelligence interest.

1. Through its requirement of a judicial warrant absent certain long-established exceptions for emergencies and arrests, the Amendment imposes a more neutral evaluation of the situation between a governmental desire for information and the action of engaging in a search. It also, equally significantly, requires a written, sworn record of the basis on which the search is undertaken.

a. It is important to emphasize, as Justice Powell did in *United States* v. *District Court*, that the fears the framers had in mind included not only invasions of privacy but also the use of a search to silence dissent.

b. The classic language here is that a detached, neutral judicial officer should stand between an over-eager executive branch and the rights of citizens.

2. The Fourth Amendment also imposes certain requirements of probable cause and sensible procedures.

a. In this area there has been a great deal of fluidity. Less probable cause is necessary if the intrusion is less or if the threatened harm is greater.

b. Such requirements as notice of the search have been held to be subject to reasonable modifications as in the case of the Wiretap Act where no notice need be given for ninety days and even then it can be delayed if this is essential to an investigation.

C. The simpler part of the question as to the impact of national security concerns on the Fourth Amendment goes to the need for a warrant at all. This part may be the more important nonetheless, for on our trust in the neutrality of judges turns a great deal of the citizens' sense of security as well as a real protection against unjustified attacks on dissent or a simple arbitrariness.

1. With the concurrence of judges from the most conservative to the most liberal wings of their benches, the courts have by now gone far toward answering the question as to the necessity for a warrant in national security areas.

a. First the Supreme Court held in a unanimous opinion by Justice Powell that the President had no power to dispense with the warrant in the area of internal security. Justice Powell emphasized the dangers to dissent.

b. Then after two courts had sustained surveillance without a warrant of diplomatic establishments and non-citizen foreign agents, the D.C. Circuit in *Zweibon* v. *Mitchell* has held unanimously that, at least wherever the party being monitored is neither a foreign agent nor a collaborator with a foreign government, a warrant is required for a wiretap even in the pursuit of foreign intelligence or foreign policy.

c. Note that this leaves the government free to search without a warrant in the cases of embassies and non-resident employees of foreign governments.

d. This area is one to be regulated by diplomacy, not by the Fourth Amendment.

2. The courts' reasoning has been, I believe, persuasive.

a. The rules as to probable cause and necessary procedures can be adjusted in such a way that the requirement of a warrant protects against malice, arbitrariness, or attacks on dissent without limiting the government in its pursuit of legitimate goals.

b. The history of the Fourth Amendment involves a number of searches in the national security area where, in important cases, warrants have been required.

c. The notion that courts are unable to understand enough of the situation to exercise a meaningful review function is implausible, especially when one recognizes that the Attorney General exercised that function for the executive branch. Moreover, there is no real risk of revealing secrets. The record of courts in this regard is far better than that of the executive branch.

d. It is my understanding that the Attorney General has now accepted the position of the D.C. Circuit at least for the time being.

3. These cases leave open three questions that the Committee could well address:

a. No court has yet held that an American citizen or resident alien—as opposed to an embassy or foreign employee of another nation—who is found to be a foreign agent or collaborator can be searched without judicially determined probable cause to believe he has committed espionage, sabotage, or some other crime. Both the Supreme Court and the D.C. Circuit have left that question open. Should there be such a category? The case against it is that the Congress has prohibited and can prohibit any conduct it considers dangerous to our national security and that no action should be taken against a citizen until there is reason to believe he has violated (or conspired to violate) such a prohibition. The case for an exception is that secret foreign agents are an important source of positive information about intentions of other governments and about other agents even when they are not yet engaged in illegal conduct.

b. If there is to be such a less-protected category of citizens who are secret agents, what should the definition of foreign agent or collaborator be when we are dealing with American citizens? It cannot, for example, open to electronic surveillance the telephones of any law firm which represents the government of France or Bolivia. A statutory definition would have to involve the secret acceptance of pay or directions from a foreign government.

c. Perhaps most important, if there is a category of American citizens who are foreign agents or collaborators and which receives less protection under the Fourth Amendment, should there not be a requirement that the status of foreign

agent or collaborator, as defined by Congress, be determined by the courts on a warrant. The excessive suspicions of Presidents Johnson and Nixon that anti-war dissent was controlled from abroad led to the CHAOS program. A sensible protection against any recurrence would be to require a judicial warrant based on a sworn affidavit establishing that a citizen is a foreign agent. This is obviously a highly important protection when organized, legitimate disagreement with government policy is involved.

D. The second aspect of the queston whether a foreign intelligence interest makes a difference to Fourth Amendment protection is harder. It raises the question whether in the case of citizens who are not foreign agents or collaborators with a foreign government there is any right to search simply to obtain foreign intelligence and not only, as traditionally, with probable cause to believe that evidence of a crime will be found. On analysis, it seems clear to me that no such right should exist, although the case law is not helpful one way or the other.

1. Put in its clearest form, the question is this. Assume that an American industrialist or banker has returned from an unfriendly country with knowledge that would be very valuable to our intelligence agencies regarding the industry or finances of the foreign country.

a. Certainly it is proper to ask the American citizen to reveal that information and indeed we presently do.

b. But what if that extremely important foreign intelligence is withheld by the citizen for any of a number of reasons. Can he then be made a subject of electronic surveillance or can his home and office be searched if the information is important enough? The question, quite starkly, is whether there should be a warrant procedure that allows searching entirely loyal Americans whenever there is probable cause to believe that they possess important foreign intelligence which they will not reveal freely.

2. I believe the answer to this question is that the matter should be handled by legislation, if at all, and not by executive discretion. Although the merits of the proposal are highly questionable, the Congress might:

a. Make it a crime to fail to turn over certain well-specified classes of information. If it did, there would then be probable cause to search for and seize such information if it was not turned over.

b. In the alternative, the Congress could make a well-defined class of information subject to subpoena.

I don't recommend either of these alternatives, but they are obviously preferable to an undefined executive discretion to search entirely loyal American citizens. If the matter is to be handled at all, it should be by legislation.

3. There is indeed case law that indicates that a search of an innocent party is improper unless there is reason to believe that the evidence will not be turned over voluntarily or in response to a subpoena. This case law would also suggest that only a well-defined class of foreign agents (who could not be expected to comply with a subpoena) might possibly be subject to electronic surveillance in order to obtain valuable, positive intelligence in situations where there is no reason to believe that they have committed or are about to commit a crime.

III. THE ADDITIONAL DIFFICULTIES PRESENTED BY THE PROGRAMS OF MAIL OPENINGS AND INTERCEPTION OF INTERNATIONAL COMMUNICATIONS TO AND FROM THE UNITED STATES AND INVOLVING UNITED STATES CITIZENS

A. Wholly aside from the special questions with regard to a possible foreign intelligence exception to the Fourth Amendment rights of American citizens, there are a series of difficult problems presented by the testimony the Committee has received with regard to mail openings and interception of international communications. I will address three of these in an order of increasing difficulty.

B. Fourth Amendment rights only pertain to American citizens in a situation where they enjoy a reasonable expectation of privacy with regard to their communications.

1. The situation with regard to mail is unusually clear.

a. The germinal case dealing with Fourth Amendment protection of the mail was *Ex Parte Jackson*, 96 U.S. 727 (1878) in which the court held that while in the first class mail, papers can only be opened and examined under a search warrant. This rule which was reaffirmed as recently as 1970 in *U.S. v. Van Leeuwen*, 397 U.S. 249, is now embodied in a federal statute, 39 U.S.C. 4057. It provides that "only an employee opening dead mail by authority of the Post

Master General, or a person holding a search warrant authorized by law may open any letter or parcel of the first class which is in the custody of the Department."

b. The only possible questions involve whether a U.S. citizen is protected as a recipient of mail from a foreign resident, or is only protected as the sender of mail. For four reasons I believe it is moderately well established that the recipient is also protected.

(1) A number of cases have indicated that there is such protection subject only to a reasonable customs power. See, *e.g.*, *U.S.* v. *Sohnen*, 298 F. Supp. 51 and *U.S.* v. *Various Articles of Obscene Merchandise*, 363 F. Supp. 165; *State* v. *Gallant*, 308 A.2d 274.

(2) 39 U.S.C. 4057 seems to clearly cover the recipient as well as the sender.

(3) The modern law with regard to the privacy of oral communications protects all the parties to the communication and would probably be read to apply to all the parties to a written communication as well.

(4) The recipient of a letter has something very close to a possessory claim to the paper on which it is written.

2. I believe the situation with regard to voice communications involving an American citizen and with one terminal in the United States is equally plainly covered both by the Constitution and by the Omnibus Crime Control and Safe Streets Act of 1968.

a. The definition of "wire communication" in the 1968 Act includes any communication made through the use of facilities for the transmission of communications by cable by any person engaged as a common carrier in providing such facilities for the transmission of foreign communications. The definition of common carrier plainly incorporates international communications to and from the United States.

b. Presumably the definition of "oral communications" would be read to be consistent with that and would therefore include radiotype voice communications.

3. The situation with regard to non-voice communications is less clear, but I believe there is every indication that they, too, would be considered protected under the Fourth Amendment.

a. As a matter of a reasonable privacy in expectation of communications, the only difference from voice communications is the extent to which a cable is revealed openly to a transmitting company. This might make revelation of its contents to the government within the reasonable expectation of senders were it not for 47 U.S.C. §605, the old Wiretap Act, which still forbids the revelation of content except "in response to a subpoena issued by a court of competent jurisdiction or on demand of other lawful authority." Any other form of interception of a non-voice communication would be a violation of a reasonable expectation of privacy. I take it that the voluntary act of a common carrier in complying with a request by a government agency to turn over cable traffic would not satisfy the exception for "demand of other lawful authority," a phrase that is apparently intended to refer to the subpoena powers granted by Congress to various agencies. See *Newfield* v. *Ryan*, 91 F.2d 700. Certainly an interception without the assistance of the common carrier would be treated as an invasion of the privacy of communications. Still, I should quickly acknowledge that there are practically no Fourth Amendment cases dealing with the interception of communications either domestically or in international traffic.

b. I do not believe that the 1968 statute covers non-voice communications. Its definition of "intercept" requires "the aural acquisition of the contents of any wire or oral communication." Acquiring the contents of a non-voice communication would not be "aural." The only possible statutory prohibition is in 47 U.S.C. § 605 which first prohibits the interception and divulgence of radio communications and then states that "no person not being entitled thereto shall receive or assist in receiving any . . . foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto."

4. With regard to each of these forms of communication, the situation may be entirely different when there are two foreign terminals.

a. A channel of communication that is overwhelmingly used and controlled by foreign interests does not invoke a reasonable expectation of privacy by American citizens.

b. The only qualification here would be if American agents or foreign governments acting at their behest specifically targeted the foreign communications of an American citizen. Here there might well be a Fourth Amendment claim.

C. In one situation the result of all this seems moderately clear. If an intelligence agency wants to open the letters or intercept the international communications of a named American citizen who is the target of an investigation, it will have to get a warrant and either show there is probable cause to believe the citizen is committing a crime or, if the Congress so determines, show that he is a secret foreign agent and that the communication is likely to contain important foreign intelligence.

1. This alone disposes of many of the situations before the Committee.

2. The lack of a clear law dealing with non-voice communications suggests that the Committee would serve a real function by addressing this question directly.

D. The hardest question arises with communications that can, without a serious invasion of privacy, be checked for words or other selection criteria or, in the case of letters, for indicators on the envelope that tend to show that the communication may contain evidence of a past or prospective crime.

1. In the case of mail, looking at the outside of the envelope for indicators that it may contain evidence is not itself a search.

2. The difficult question arises if it turns out that the indicators will lead the investigative agency to read a number of innocent letters for each letter that contains evidence of a past or prospective crime. At this point, there is apparently no choice other than to either open the letter and invade the privacy of the sender and receiver or to leave it unopened although there is a probability that it contains evidence bearing on a substantial danger.

a. In traditional terms, the question is one of a general search. The Constitution was written to forbid general search warrants such as the Writs of Assistance were in colonial times.

b. There is no simple answer to when a search is too general. Any search involves a certain probability that it will not reveal evidence and every search, even where the result is that evidence is found, involves breaching the privacy of non-evidentiary matters. The question is always one of establishing a balance between the invasion of privacy and the need for the search. As always under the Fourth Amendment, if what is involved is a serious prospective crime, there is more room for a fairly general search.

3. The problem with international communications is similar, but may be subject to more of a technological solution. Consider the case of non-voice communications between an American citizen and an alien.

a. General Allen's testimony indicates that it may be possible to identify certain selection criteria without reading the entire message. These, like the indicators on the outside of a letter, would narrow the number of communications inspected and would increase the probability that any single communication contained evidence of a past or prospective crime. If this were done mechanically without reading all of the messages, there would not be a search during this stage of the operation.

b. When a narrower, but perhaps still excessive, class of non-voice communications has been identified, it may be possible to review these without revealing the name of the sender or receiver. Adding in that second step would substantially reduce the invasion of privacy.

c. It is also, of course, relevant whether the intelligence agency immediately discards any message that, on reading, proves to be innocent without keeping copies or records of the transactions.

4. The hardest question of all would be presented if: (1) an important part of the communications traffic on an international route to and from the United States does not involve American citizens; and (2) there is no way of sorting this part of the traffic from the part involving American citizens without a substantial invasion of the privacy rights of citizens. This might well be true with regard to voice communications, for example. Here there would be two questions to be addressed in sequence.

a. What procedures could be developed to minimize the intrusion on the privacy of American citizens, for example by quickly and completely discarding any communication involving American citizens and not revealing evidence of a crime?

b. What is the balance between the now-diminished invasion of the privacy of American citizens and the volume and importance of the purely foreign traffic involved? If, for example, ninety-five percent of the "take" were domestic and the remaining five percent pertained primarily to commercial matters, the balance would have to be struck in favor of forbidding the particular technique of intercepting international communications.

E. Obviously the questions I have just reviewed concerning the permissible techniques for monitoring international communications are matters which badly need legislative standards. In some cases, the nature of the program will be so clear and stable that Congress could itself define the requirements. In other cases, the Committee might well wish to consider a warrant requirement that first set forth general standards and procedures and then directed a court to approve a broad plan for monitoring a particular type of communications.

1. In either event, I would think it was highly desirable to require the intelligence agency to furnish on a continuing basis two forms of information.

a. Copies of any communications perused in their entirety with some indication of which ones were furnished to other government departments.

b. A numerical summary of the relationship between communications read but discarded and communications read and kept as part of any governmental program or file.

2. This will make it possible to estimate the extent to which the search is over-broad, the equivalent of a general warrant.

TESTIMONY OF PHILIP B. HEYMANN, PROFESSOR OF LAW, HARVARD LAW SCHOOL

Mr. HEYMANN. Mr. Chairman, I recognize it is late, and if I could submit my prepared statement for the record, I would be happy to try to summarize in a very few minutes what I have to say.

My objective, Mr. Chairman, is to try to state clearly the four or five or six issues that I think are presented by surreptitious entries, domestic bugging, NSA interceptions and mail openings.

I have had the feeling today that sometimes we are dealing with a large ball of wax called national security; sometimes we are dealing with 500 difficult little issues. My own view, and I hope I can convince you, is that there are about five or six different issues, and that this committee can address them individually with the result, I hope, that the law will be a little clearer when you are through. There are two types of issues. I want to break the categories into two, and then break them. There are certain issues that go directly to what the impact of foreign intelligence is on fourth amendment rights. Then there is another set of issues that involve what is special about international communications, mail, nonvoice cable, or voice.

Let me start with the question of what is special about national intelligence, foreign intelligence, because that one cuts through everything this committee has looked at. It cuts all the way from black bag jobs to sophisticated NSA items.

As you well know, there are two primary protections here, and foreign intelligence considerations could affect these. First, the fourth amendment has a warrant protection, to get a judge over an overly eager executive branch, if it is over-eager in a search. The warrant was there largely, as Justice Powell reminded us recently, because of fears as far back as the 18th century.

In the area of the warrant, the first part of what is special about intelligence, the courts have taken us a very long way toward a conclusion. First the Supreme Court, in the *United States* v. *U.S. District Court*, held that internal security required a warrant. Then the D.C. Circuit, in *Zweibon* v. *Mitchell*, in an opinion that the Attorney General has said he will live with, at least for the time being, has said even when the Government is pursuing foreign intelligence, it must get a warrant unless it's dealing with a foreign agent or collaborator. In other words, a great deal of the ambiguity the Congress left in

1968 is now cut down to the question, what happens with foreign agents and collaborators. As to that, I think that this committee has two very important questions to address, and it has been asking them of the Attorney General today. One question is: What should the definition of foreign agent or collaborator be? Senator Hart was pressing the Attorney General on that. It is not going to be an easy thing to draw up. If there is some special category of foreign agent and collaborator, it is going to take some work. It cannot include New York law firms who are representing Bolivia or France. It cannot include major Jewish organizations working in collaboration with Israel on a bond drive. It is going to take some work.

The second issue under the warrant that this committee is going to have to address is: If there is an exception for foreign agents and collaborators, should that be decided by the executive branch without a warrant, or should there be a warrant required where a judge decides that someone is a foreign agent, a citizen, a foreign agent or collaborator? Let me be clear that no one, including me or any court, is suggesting a warrant requirement for embassies or nonresident employees of foreign governments, all right? But what if the executive branch believes that someone is a foreign agent or a collaborator? Should not a court have to get into it? I would strongly urge that they should.

The CHAIRMAN. Are you talking in this point, Professor Heymann, about bugging and wiretapping? The cases you have cited relate to those traditional methods.

Mr. HEYMANN. I believe exactly the same standard would apply with regard to intercepting overseas communications, Senator Church. In other words, as I go about three steps down the line I am going to say to you that I think it is clear that international mail with a U.S. terminal, or U.S. citizen; international phone conversations, the same conditions; and international cable traffic, are all protected by the fourth amendment. I am going to give you cases and statutes that say that, and I am going to say that requires a warrant unless it is a foreign agent.

I hope that this committee says if the Government wants to say it is a foreign agent, it will require a warrant to certify that it is a foreign agent.

The second half of what is special about foreign intelligence is do you always need probable cause of crime, or can the Government sometimes go out, simply pursuing foreign intelligence. I think that you have to divide that one into two cases. One, with regard to foreign agents or collaborators, it makes some sense. There is a quite arguable position that for a foreign agent or a collaborator so certified by a court on a warrant, the Government ought to be able to pursue foreign intelligence, not just probable cause of a crime. The executive branch could live with a stricter standard, but there are cases that you can imagine and point out where a foreign agent would have information about a foreign country's plan that you wanted to pick up, with or without probable cause that the agent is committing a crime; or a foreign agent would make contact with other agents whose names it was important to know.

My sharpest difference with everything that the Attorney General was saying comes, I think, in the question, can the Government pick

up information from loyal, trustworthy American citizens by electronic surveillance at home, or through international means? Can it do that simply to get foreign intelligence when there is no evidence of a crime? Let me state the question very specifically: if David Rockefeller goes to the Soviet Union and learns information about their financial structure that the CIA would give a great deal to know, that it is very important to our foreign security, is there a right to bug David Rockefeller's phone to find out what he has learned? At the moment, as you know, we do make inquiries of David Rockefeller, and that is entirely proper. The question is if for any of a number of reasons he refuses to furnish that information, the foreign intelligence information that the executive branch wants, can his communications be monitored to find it out?

The CHAIRMAN. At home?

Mr. HEYMANN. I mean at home, by cable overseas, letter overseas. I mean by phone overseas, Mr. Chairman. It seems to me that the Congress has to face up to that rather directly.

The CHAIRMAN. Let us take the case of business transactions that may have an economic impact upon the United States. I would take it that if they were a transaction that involved foreign governments, investments, capital transfers and the like, that this would be within the right of the Government to obtain information through electronic surveillance methods, or any other method.

Mr. HEYMANN. The position that I am urging on you, Senator——

The CHAIRMAN. We are talking now about actions of foreign governments in the economic field.

Mr. HEYMANN. The question is whether the communications of an American citizen are monitored secretly to find out that information. I suggest to you that Congress would not pass a statute making it a crime to withhold valuable information, making it a crime for an American citizen to withhold valuable information, that Congress would probably not pass a statute authorizing an executive agency to subpena that information. It would be regarded as the information of that citizen. If Congress were not to allow it to be done directly by criminal statute or subpena, Congress should not allow it to be done indirectly by the executive branch monitoring an entirely innocent American citizen's communications.

The CHAIRMAN. Suppose that you are looking simply for intelligence having to do with messages of foreign governments.

Mr. HEYMANN Wholly?

The CHAIRMAN. You would have no problem with that?

Mr. HEYMANN. Foreign to foreign messages, I would have no trouble with, and foreign to foreign terminals, I have no trouble with.

The CHAIRMAN. How about messages between foreigners, as such, either abroad with both terminals abroad, or one terminal in this country and the other terminal abroad? Any trouble with that?

Mr. HEYMANN. Between two foreigners?

The CHAIRMAN. Yes.

Mr. HEYMANN. No, Mr. Chairman. There could be possibly a problem with resident aliens, but setting that minor problem aside——

The CHAIRMAN. Suppose in order to get the messages of foreign governments or foreign aliens with which you would have no problem,

it was necessary for technical reasons to take these messages out of the whole stream of messages.

Mr. HEYMANN. That is the hardest problem of all, Mr. Chairman.

The CHAIRMAN. Yes, it is.

Mr. HEYMANN. If I just may take three sentences to work up to the hardest problem. As I said to you, my statement makes clear that I think the law is absolutely solid that letters, including international letters, are protected. They have been protected by statute of Congress since 1825. The Supreme Court has held them highly protected for the last 80, 90 years. I think the law with regard to international voice communications involving American citizens is clear, constitutionally protected, and protected under the Safe Streets and Crime Act. I think the Wiretap Act applies to international communications if you look carefully at its definitions.

Mr. SCHWARZ. Do you mean with one terminal in the United States?

Mr. HEYMANN. With one terminal in the United States, that is the way the definition was.

Finally, I think the case is slightly less clear in regard to nonvoice communications. What this means, the second sentence that leads up to your hardest of examples, if these are protected communications, then you need a warrant. I think the Attorney General agrees with that, although he is hard pressed to say at this time, November 6, whatever date it is. If these are protected communications, the executive branch cannot read them or hear them without a warrant if what is being read, if what is being targeted is an American citizen. If somebody says I want to read Frank Church's international cables, there is a warrant requirement protecting it.

The hardest question, if what is being targeted is not an individual American, if it is an individual American——

The CHAIRMAN. To answer my question.

Mr. HEYMANN. That is the hardest question. As your committee has heard, the NSA has systems for identifying particular parts of the international traffic which are somewhat more likely to contain either evidence of a crime or foreign intelligence information than other parts. What if once it has identified a large, relatively large volume of traffic, that is suspicious? It will still be true that the investigating agency is going to have to read a great deal of that traffic in order to separate out perhaps perfectly proper foreign-to-foreign cables from American cables. Then what? My answer is really quite similar to the Attorney General's, if I heard him right, Mr. Chairman. The first question is what steps can be taken to minimize the invasion of privacy with regard to the protected cables involving an American citizen, an American terminal, or a protected phone conversation or protected mail? What steps can be taken to minimize the invasion? That includes, among other things, how quickly is the matter discarded, who sees it.

The second step which I think the Attorney General recognized this morning is you then compare the minimized—a court would have to and the Congress would have to—the minimized damage to American privacy with the importance and the value of the foreign-to-foreign traffic which is intercepted. If it turns out that 95 percent of the traffic is protected in the sense that it involves a loyal American citizen as one terminal in the United States, and 5 percent is foreign to

foreign, and the 5 percent is not of great value, say the 5 percent involves the price of grain; then the whole bundle would be unconstitutional.

THE CHAIRMAN. Who makes that judgment?

Mr. HEYMANN. The last question. It can only be done in one or two ways, I believe. If we are talking about a type of interception of communications which was very constant over time, Congress could go far to either declaring it legal or illegal. If we are talking about a type of interception that may change and be different next year than it is this year, Congress is going to have to lay down standards for courts to apply.

Now the Attorney General's statement this morning contains references to a number of cases where the Supreme Court has ordered and authorized courts to set up general principles and general procedures for handling fourth amendment questions. The most recent is Justice Powell involving Customs searches on the border of Mexico. The Supreme Court with Justice Powell speaking said, the lower court ought to say just when and where there can be inspections within 20 miles of the border of Mexico.

I believe that ultimately the Congress is going to have to pass a statute that sets forth standards and then requires a warrant from a court. Perhaps a warrant approving a monitoring system with a whole volume of traffic. It does not have to be a warrant for each individual bit. Congress is going to have to set forth the standards and courts are going to have to come in and apply them.

Finally, I think it is very important that the whole system is not going to work unless there is some what is technically called feedback where the court or legislative oversight committee keeps getting records regularly giving a comparison of the quantity and quality of the American messages being intercepted, the innocent American messages being intercepted, a comparison of that quantity and quality with the value of the legitimate take. There is going to have to be some sort of system that keeps bringing that back in.

The CHAIRMAN. It would seem to me that where you get into the legitimate foreign intelligence area that the introduction of a court device or the warrant device may indeed become very awkward. The best device would be an oversight committee of the Congress that would be kept fully informed and would pass judgment on these cases just to satisfy itself that these operations were being kept within proper guidelines and under proper restriction.

The trouble I have with the Attorney General's dissertation and his responses today is that he somehow seems to visualize that all of this could be done within the executive branch, that everything could be worked out with better procedures. Unless there is somebody checking on the executive branch that is not part of the executive branch and not subject to the ultimate control, direction and dismissal of the President, I do not think you have much protection.

Mr. HEYMANN. I certainly agree with that, Mr. Chairman. The only thing that I question in your statement is to whatever extent it involves a notion that entirely innocent, meaning nonforeign agent, American citizens can properly be monitored in their communications at home or from home to abroad simply because they are thought to possess in their minds intelligence which the CIA, or the NSA, or the State Department, or the Department of Defense, or the White House

would like to have. That is a notion which I believe on reflection the committee will find unpalatable. I must say I believe that, and a number of courts have acted whether it is in dictum quite acceptable. On reflection courts will not accept it. I think when the committee thinks hard about what it means——

The CHAIRMAN. In such cases you would require a warrant, or would you simply flatly prohibit?

Mr. HEYMANN. I would simply flatly prohibit a claim to own the mental——

The CHAIRMAN. That would be part of the definition. That would be part of the statutory exclusion from a definition of foreign intelligence.

Mr. HEYMANN. That is correct. In fact, the amendment that was written in 1789 or 1791 requires probable cause. Of course it has been extended and applies otherwise now.

The CHAIRMAN. Mr. Schwarz would like to ask a question.

Mr. SCHWARZ. Picking up on Senator Church's and your recognition of the hardest question, on a stream of communications, I understood your first point to be that if upon analysis the foreign intelligence value of the stream is not very great, even though it might exist, you say the stream could not be surveilled at all.

Mr. HEYMANN. If surveilling the stream requires a substantial invasion of the privacy of protected American communications.

Mr. SCHWARZ. Now let us assume that the stream does include significant, legitimate foreign intelligence—government to government—and in the course of analyzing, of obtaining that, it is technologically inevitable that one also obtains American citizens' messages. I want to put two different cases to you. One of those messages from an American citizen to an American citizen upon analysis contains evidence of a crime, although no one had any reason to suspect that before the stream was interrupted. The other message contains evidence of either economic matters or political matters. What do you do with those two messages that NSA or some other agency has now? Under your first principle, it was legitimate for the NSA to surveill the stream, and in the course of doing so it has acquired these two messages. What should they do with them?

Mr. KIRBOW. This is without a warrant?

Mr. SCHWARZ. There has been no warrant.

Mr. HEYMANN. My answer, Mr. Schwarz, is the traditional one. I believe it is the opposite of what the Attorney General suggested today. I think if the NSA legitimately reads a message which revealed itself as being evidence of a crime, keeps that message and seizes it, it has come upon it legitimately and is evidence of a crime. It keeps it and uses it and sends it to the FBI and it sends the people to jail. The other message that it reads that involves economic information, it has no right to. That is what I was urging upon Senator Church. That you have no right to take from American citizens what they happen to know just because the Government is interested in it, too.

One of my major differences with the Attorney General this morning was the notion that the fourth amendment particularly protects criminals, that its most important function is to exclude evidence against criminals. It was not written for that. It was written to protect

you and me. In your case I would send it directly to the FBI. I would send the message that indicated evidence of crime.

Mr. SCHWARZ. That you would send to the FBI, but the one economic or political——

Mr. HEYMANN. Would have to be destroyed immediately.

Mr. KIRBOW. Where do you attach the illegality? At the collection point, or the distribution point, or the machine where they supposedly sort all of this you are talking about?

Mr. HEYMANN. Let me take it in those three stages, Mr. Kirbow. I do not think that there is any search that is worth being called a search that would trouble anybody, either in looking at the envelopes for indicators, whatever they may be. I do not know what they are, or in going through voice or nonvoice traffic simply to cut down from 1 million items to 100,000 items which have the word assassination in them, let us say, or have the word North Korea in them. I do not think there is any search running those million items past somebody, only going so far. That does not seem to be a search.

The next step is the question as to whether you then have to read the 100,000 items along with the name of the sender and receiver. If it were technologically possible to do this somehow or another without getting the name of the sender and receiver, you could read the items. I think that there was just a limited search at the second stage. But if at the second stage, having cut yourself down to envelopes with indicators or some other kind of international traffic with selection criteria, if at that point you have to read the whole message or hear the whole message, together with the sender and receiver, there is very definitely a search at that point. You can minimize the effect of the search by thereafter discarding quickly whatever you have no right to.

Mr. KIRBOW. Do you mean to draw a distinction between reading the body of the message which I send as being different from one which I send if you read my signature as the sender and the addressee as the receiver? Do you draw a distinction between those two categories?

Mr. HEYMANN. I recognized it is idiosyncratic. I have not seen it anywhere else. When I think of it myself, I think I would feel quite differently. Let us take a letter, for example, about having a Government official read my letter, the body of my letter. If it were possible to eliminate who wrote it and who it is to, I would feel very differently about the privacy of that letter from a Government official reading it and knowing who it is from and who it is to.

Mr. KIRBOW. You are familiar with some of the technology of extremely high-speed transmissions, are you not? How do you distinguish there where they are almost instantaneously sent and then the signal goes off the air, and in that stream or volume of information when they are finally decoded on the other end, or smoothed out on the other end, we will call it by another mechanical device? How do you provide for such high-speed transmissions in this theory of yours as to what is legal? These are messages which make nothing but a sound as they go out over the air as you probably know. What do you do with those sort of things, which is the predominant way of sending secret information?

Mr. HEYMANN. I just have to go through the steps, Mr. Kirbow. There is no happy answer at the end of the steps. The first question is you have to identify conceptually what it is legitimate to pick up and

what it is not legitimate to pick up on that instantaneous stream, almost instantaneous stream. I have argued it is only legitimate to pick up foreign agents' traffic, foreign to foreign traffic, evidence-of-crime traffic, or something like that. First you have to identify what is illegitimate and what is legitimate. Then you ask yourself, is there any way that you can process this stream so to cut down the invasion of privacy to a minimum in the legitimate traffic that should not be intercepted?

You know, in the protected traffic, once you have done that and you explore every possibility for doing that, you do it by statute or by warrant. The next step is to say what is the balance between what is properly taken out of that and what is not? I agree with you. I think you are suggesting, Mr. Kirbow, when you are all through with that kind of fancy transmission, you're going to have a lot of useless stuff that you are allowed to take and a lot of stuff that you are not allowed to take when you are all through. At that point Congress and the courts are going to have to decide whether you are getting too much that is protected in order to get what you are legitimately allowed to take.

Mr. KIRBOW. Among the methods being used I do not see when the production comes you can review it as an aftereffect thing. I do not see how you are protecting the sender and receiver from an interception of the communication.

Mr. HEYMANN. I would require some kind of warrant in advance, unless Congress could handle that by statute, which I do not think the warrant procedure—I am shooting a little bit from the hip, Mr. Kirbow. I have only been thinking about it in the last few days since I started looking into it. The warrant procedure might say a court would itself pass on the selection criteria and the Congress might say use qualitative standards, saying the selection criteria should only be acceptable if they are so designed as to bring in highly important information of a foreign intelligence sort, proportionate in some way to the invasion of privacy. Then it could go on and Congress could add a second paragraph and say, even with these selection criteria, it can only be used if the following measures and minimization are used. Something like that.

Mr. KIRBOW. Thank you.

The CHAIRMAN. I think that we all recognize that this is a very complex matter when we are dealing with such advanced and rapidly changing technologies, and it leaves us all groping for new ways to keep old protections alive.

I think that your testimony has been very forthright and it has been very helpful. I want to thank you for it.

Mr. HEYMANN. Thank you very much.

The CHAIRMAN. That concludes the hearing today. We meet again in a public session at the call of the Chair.

[Whereupon, at 4:25 p.m., the hearing in the above-mentioned matter was concluded.]