WARRANTLESS WIRETAPPING

HEARINGS

BEFORE THE

SUBCOMMITTEE ON
ADMINISTRATIVE PRACTICE AND PROCEDURE

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

NINETY-SECOND CONGRESS

SECOND SESSION

ON

PRACTICES AND PROCEDURES OF THE DEPARTMENT OF JUSTICE FOR WARRANTLESS WIRETAPPING AND OTHER ELECTRONIC SURVEILLANCE

JUNE 29, 1972

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
93-045 WASHINGTON : 1973

COMMITTEE ON THE JUDICIARY

JAMES O. EASTLAND, Mississippi, *Chairman*

JOHN L. McCLELLAN, Arkansas
SAM J. ERVIN, JR., North Carolina
PHILIP A. HART, Michigan
EDWARD M. KENNEDY, Massachusetts
BIRCH BAYH, Indiana
QUENTIN N. BURDICK, North Dakota
ROBERT C. BYRD, West Virginia
JOHN V. TUNNEY, California

ROMAN L. HRUSKA, Nebraska
HIRAM L. FONG, Hawaii
HUGH SCOTT, Pennsylvania
STROM THURMOND, South Carolina
MARLOW W. COOK, Kentucky
CHARLES McC. MATHIAS, JR., Maryland
EDWARD J. GURNEY, Florida

SUBCOMMITTEE ON ADMINISTRATIVE PRACTICE AND PROCEDURE

EDWARD M. KENNEDY, Massachusetts, *Chairman*

PHILIP A. HART, Michigan
BIRCH BAYH, Indiana
QUENTIN N. BURDICK, North Dakota
JOHN V. TUNNEY, California

STROM THURMOND, South Carolina
CHARLES McC. MATHIAS, JR., Maryland
EDWARD J. GURNEY, Florida

JAMES F. FLUG, *Chief Counsel*
MICHAEL T. EPSTEIN, *Assistant Counsel*
HENRY HERLONG, *Minority Counsel*
CAROLINE J. CROFT, *Staff Member*

CONTENTS

EXHIBITS

PRACTICES AND PROCEDURES OF THE DEPARTMENT OF JUSTICE FOR WARRANTLESS WIRETAPPING

THURSDAY, JUNE 29, 1972

U.S. SENATE,
SUBCOMMITTEE ON ADMINISTRATIVE PRACTICE AND PROCEDURE
OF THE COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:40 a.m., in room 6202, New Senate Office Building, Senator Edward M. Kennedy (chairman of the subcommittee) presiding.

Present: Senators Kennedy (presiding) and Hart.

Also present: James Flug, chief counsel; Michael T. Epstein, assistant counsel; and Henry Herlong, minority counsel.

Senator KENNEDY. The subcommittee will come to order.

I appreciate the patience of the witnesses this morning. I was testifying at the Foreign Relations Committee and they were a little late getting started.

On August 1, 1971, Attorney Lewis Powell, in a newspaper article, wrote the following:

> The question is often asked why, if prior court authorization to wiretap is required in ordinary criminal cases, it should not also be required in national security cases. In simplest terms the answer given by the government is the need for secrecy . . . Court authorized wiretapping requires a prior showing of probable cause and the ultimate disclosure of sources. Public disclosure of this sensitive information would seriously handicap our counter-espionage and counter-subversive operations.

Citing no basis for this finding, he then concluded, "The outcry against wiretapping is a tempest in a teapot . . . Law abiding citizens have nothing to fear."

On June 19, 1972, Mr. Justice Lewis Powell, having read the briefs on both sides, having seen the records of 14 months eavesdropping on a security tap, and having heard oral arguments in the *Keith* case (*U.S.* v. *U.S. District Court et al*), wrote the following:

> The danger to political dissent is acute where the government attempts to act under so vague a concept as the power to protect domestic security. Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent.

And in one of the most stirring judicial statements of our times, he concluded:

> The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of government action in private conversation. For private dissent, no less than open public disclosure, is essential to our free society.

I cite at length the trend in Lewis Powell's statements because I think he would be the first to say that they set the pattern for the change that is required right now in the Justice Department's approach to wiretapping and bugging of Americans, especially dissenting Americans. Attorney Lewis Powell's 1971 views closely tracked—and cited—those of John Mitchell and his Department. Mr. Justice Powell's 1972 views on behalf of the Supreme Court, and without dissent, are now the law of the land. They must be followed in letter and in spirit by those who have sought to eavesdrop, without limit or review, on our citizens in their homes and offices and gathering places. The time for playing fast and loose with the Bill of Rights has come to an end.

Our goal here today is to relieve all Americans of that "dread of unchecked surveillance power" and that "fear of unauthorized official eavesdropping", by having the Justice Department make clear its commitment to change its ways not only in form but in substance. For unless the Department truly adopts as its own the Supreme Court's heavy emphasis on first and fourth amendment rights, the *Keith* opinion will become a fraud upon the Nation's citizens, a bare judicial promise of constitutional protection, but a promise that can be broken by the performance of the executive branch.

We are here to see that the constitutional promise is kept, that our right to be let alone, our right to privacy, our right to speak freely in public and in private, our right to have different views, and the other rights which keep our lives free from unwarranted government intrusion, are vindicated rather than evaded, preserved and not avoided, enhanced instead of circumvented.

Attorney General Kleindienst was quoted last weekend as saying that he disagreed with the Supreme Court's holding that his Department must obtain judicial warrants to tap and bug in the interest of domestic security. But fortunately, as I am sure he would agree, his sworn duty is to uphold the constitution as interpreted by the Supreme Court, regardless of his personal preferences. I am confident that he shares the views that nothing undermines respect for our legal system more than lawlessness by lawmen, and that—especially when interference with fundamental freedoms is at stake—official lawlessness cannot be tolerated or condoned.

Some facets of the *Keith* opinion are not yet clear, as we shall see this morning. But certain basic facts are clear:

1. Warrantless tapping and bugging of purely domestic organizations and individuals should have ceased on June 19.

2. Although the Court thinks Congress could set forth different warrant procedures and standards for so-called domestic security eavesdropping, the only statutory basis for issuing any warrants at present is title III of the 1968 law, with all of its limitations and requirements fully applicable.

3. The Court specifically did not decide whether warrantless tapping and bugging is permitted with respect to the activities of foreign powers; nor did it define the degree of collaboration between a domestic group and a foreign power which would turn a domestic group's behavior into foreign unlawful activities which might be subject to different surveillance rules. However, the Court clearly

rejected title III as a source of affirmative authority for any warrantless installations and clearly rejected the Department's arguments against judicial involvement in so-called national security cases. Thus the Department is plainly on notice that the key underpinnings of its position, even on purely foreign targets, have been removed and that it continues its practices in this field at its own risk.

4. The Court has clearly placed a heavy presumption in favor of the protection of fourth and first amendment rights as against asserted security needs, and that presumption applies equally to a decision whether to install a warrantless device on a foreign subject, or deciding what procedures apply to a domestic group with foreign contacts, or determining whether to seek to eavesdrop at all on a domestic group. In other words, whatever the dividing lines used to be between spying and not spying on people electronically, that dividing line has been moved significantly in the direction of not spying.

Our witnesses today will provide us with a variety of viewpoints on the implications of the Supreme Court's opinion.

Deputy Assistant Attorney General for Internal Security Kevin Maroney was suggested personally by Attorney General Kleindienst as the Department's representative at today's hearing, and we have been assured that he is in possession of all the facts and fully authorized and prepared to speak in detail on behalf of the Department on the vital matters before us.

Former Attorney General Ramsey Clark has very graciously rearranged his busy schedule to be here today to give us the benefit of his experience with national security wiretapping, the procedures which control it, its utility, and its problems.

Former Assistant Solicitor General Nathan Lewin is here to provide an independent legal view of the meaning of the decision, and to analyze the probable course that the Court may take henceforth and the implications of that projection.

Today's hearing is not designed to deal comprehensively with all of the remaining problems and prevailing practices in the field of security eavesdropping. We hope to meet that need at later hearings. Today's session will, however, meet the immediate need to reassure the American people that the Justice Department knows that the constitution means what the Supreme Court says.

[The complete text of the Supreme Court, opinions in the *Keith* case appears at page 183. The complete text of the Federal Wiretapping status appears at page 183.]

I would like to welcome our first witness, Kevin Maroney of the Department of Justice.

Mr. Maroney is Deputy Assistant Attorney General of the United States for Internal Security. As I said, Mr. Maroney was recommended to us for these hearings by Mr. Kleindienst.

I want to welcome you here today. I understand you have a prepared statement.

TESTIMONY OF KEVIN MARONEY, DEPUTY ASSISTANT ATTORNEY GENERAL FOR INTERNAL SECURITY, DEPARTMENT OF JUSTICE

Mr. MARONEY. Thank you, Mr. Chairman.

Mr. Chairman. I am happy to appear here today on behalf of the Department of Justice in response to your request for our views on the subject of electronic surveillance and in particular, concerning the impact of the Supreme Court's decision last week in the case of *United States* v. *U.S. District Court for the Eastern District of Michigan*, No. 70–153 decided June 19, 1972, and more popularly known as the *Keith* case.

The immediate impact of the *Keith* case was set forth clearly by Attorney General Richard G. Kleindienst in his statement of June 19, 1972. Let me quote:

> In accordance with the decision of the Supreme Court, I have today directed the termination of all electronic surveillance in cases involving domestic security that conflict with the Court's opinion. Hereafter, surveillance will be undertaken in domestic security cases only under procedures that comply with the Court's opinion.

Senator KENNEDY. Now, just at this point where Mr. Kleindienst said, "In accordance with the decision of the Supreme Court, I have today directed. . . ."

Whom did he direct with respect to the termination of all such electronic surveillance?

Mr. MARONEY. The FBI.

Senator KENNEDY. What procedures were to be followed by the FBI in making decisions whether the taps that they were operating fell within the purview of the *Keith* decision? Was there an outline of any kind of procedures? How was it left?

Mr. MARONEY. A review was made by the Attorney General of all the electronic surveillances which were then in place in light of the information which had been submitted to him in connection with the request for the initial installation. Based on that factual information and applying the standards of the *Keith* decision, the Attorney General directed that certain of those installations be removed, since they were covered by the prohibition of the *Keith* case.

Senator KENNEDY. Who applied the standards of the *Keith* decision? Who made those decisions? Was that the Attorney General himself?

Mr. MARONEY. Made by the Attorney General in consultation with the Assistant Attorney General of the Internal Security Division.

Senator KENNEDY. Well, who looked at the facts regarding each tap?

You see, there now is a Supreme Court decision setting up some standards, and I want to find out how you have been applying those standards to the actual taps that have been on. Is it the Attorney General himself who has been reviewing all the facts? Is he the one who has been deciding which taps fail to meet the standards and that therefore they should be lifted? Or are you telling the head of the FBI to do that? If you are telling the FBI to do that, then we want to know what procedures you have formulated. We want to know who has the authority and what instructions he has received from the Attorney General.

Mr. MARONEY. The legal decision as to the applicability of the *Keith* decision to installations that were then in place was made by the Attorney General in consultation with the Assistant Attorney General in charge of Internal Security based on the factual information which they had.

Senator KENNEDY. Does that mean that the two of them reviewed the facts in each case, or did the Attorney General just give that authority to the Assistant Attorney General?

As I indicated before, we want to know what procedures are being used within the Justice Department to implement this decision. The fact that someone is being directed is fine. But we want to find out how he was directed, what direction and guidance he received, and who actually makes the decision. Is it the Attorney General himself?

Mr. MARONEY. The Attorney General personally makes the determination based on the facts available to him. In the first instance, when a request is made for authorization to install an electronic surveillance, and in this particular instance, in light of the Court's determination in *Keith*, that was a legal determination by the Attorney General based on the facts available in the Department.

Senator KENNEDY. Well, did he review each of the factual situations himself?

Mr. MARONEY. He reviewed the installations in light of the facts known to him; yes, sir.

Senator KENNEDY. Well, how would he know the facts unless he reviewed each of the factual situations himself?

Mr. MARONEY. Well, of course, the Attorney General has a factual background in each of these instances. He has to make that review before it is placed on in the first place.

Senator KENNEDY. Okay, but it was he who made the decisions with regard to the terminations.

Mr. MARONEY. Yes.

Senator KENNEDY. He did that himself?

Mr. MARONEY. Yes, in consultation with the Assistant Attorney General.

Senator KENNEDY. He did that himself and he made the judgments himself after consultation?

Mr. MARONEY. Yes, sir. All these determinations are made personally by the Attorney General.

Senator KENNEDY. On each of the taps?

Mr. MARONEY. Yes, sir.

Senator KENNEDY. All right.

Then with respect to the sentence, "I have today directed the termination of all electronic surveillance in cases involving domestic security that conflict with the Court's opinion," it was the Attorney General himself who made the determination which taps conflicted with the Court's opinion?

Mr. MARONEY. Yes, sir.

Senator KENNEDY. The Attorney General's statement then said, "Hereafter, surveillance will be undertaken in domestice security cases only under procedures that comply with the Court's opinion."

Does that mean a warrant?

Mr. MARONEY. A warrant procedure, yes, sir.

Senator KENNEDY. All right. We will come back to that.

Mr. MARONEY. Whatever problems, Mr. Chairman, some may have had with respect to the difficult issue of electronic surveillance involving wholly domestic organizations have, in great part——

Senator KENNEDY. Excuse me for another interruption here about that quotation from the Attorney General's statement. The next paragraph of the Attorney General's original release stated:

> The Court invited Congress to legislate the standards and procedures for court-approved electronic surveillance in such cases—as Congress already has done in criminal cases.
>
> Therefore, I am also directing the appropriate officers of the Department of Justice to work closely with Congress in formulating legislative standards for domestic security surveillance.

Could you tell us where that stands now? The Attorney General said, "I am directing appropriate officers.***" I imagine that includes you.

You see, your statement didn't include the next two paragraphs that were in the Attorney General's statement.

[The complete text of the Attorney General's statement of June 19, 1972 follows:]

DEPARTMENT OF JUSTICE

JUNE 19, 1972.

Attorney General Richard G. Kleindienst issued the following statement today:

In accordance with the decision of the Supreme Court, I have today directed the termination of all electronic surveillance in cases involving domestic security that conflict with the Court's opinion.

Hereafter, surveillance will be undertaken in domestic security cases only under procedures that comply with the Court's opinion.

The Court invited Congress to legislate the standards and procedures for court-approved electronic surveillance in such cases—as Congress already has done in criminal cases.

Therefore, I am also directing the appropriate officers of the Department of Justice to work closely with Congress in formulating legislative standards for domestic security surveillance.

It should be noted that the Court's opinion was confined to the narrow issue of the use of electronic surveillance in domestic security cases, and it does not affect the use of electronic surveillance for the gathering of foreign intelligence in national security matters.

The Internal Security Division is reviewing pending cases to determine the effect of the opinion and will make recommendations to me on whether to disclose information obtained by electronic surveillance to defendants or to dismiss the charges against them.

Mr. MARONEY. Oh, I see, you are reading from the Attorney General's press release?

Senator KENNEDY. That is right. In your prepared statement, you quoted from the Attorney General's June 19 press release, and I was reading the next two paragraphs of that release.

Do you want to take a look at our copy of the release?

Mr. MARONEY. No, I have it.

Senator KENNEDY. Those two paragraphs state:

> The Court invited Congress to legislate the standards and procedures for court-approved electronic surveillance in such cases—as Congress already has done in criminal cases.
>
> Therefore, I am also directing the appropriate officers of the Department of Justice to work closely with Congress in formulating legislative standards for domestic security surveillance.

Is that process going on now?

Mr. MARONEY. No, sir. As I indicated in my statement, for the present, we have decided not to seek amendatory legislation and to let the experience of the next months indicate whether or not there appears to be a legal void which we might suggest to the Congress for amendatory legislation. But for the moment, we do not intend to seek amendatory legislation and to let the experience of the next months indicate whether or not there appears to be a legal void which we might suggest to the Congress for amendatory legislation. But for the moment, we do not intend to seek such amendatory legislation from the Congress.

Senator KENNEDY. Why did the Attorney General change his mind? He said in his June 19 press release that the Justice Department was going to work with the Congress in accordance with the Invitation by the Court. Why the change now?

Mr. MARONEY. Well, we initially started on the preparation of, or at least looking at the possibility of draft legislation in light of the language in Justice Powell's decision. However, it was subsequently determined by the Attorney General that we would not at this point seek such legislation, we would let experience dictate the needs in the light of the requirements of the decision.

Senator KENNEDY. I know that you have read Justice Powell's opinion. Did it not appear to you that the Court was inviting Congress to legislate in this area? What is the administration urging the Congress to do? Do you want us to legislate in this area or not? We have been invited by the Court to do so.

Do you want us to legislate at all?

Mr. MARONEY. At this time, Mr. Chairman, we are not requesting any legislation; we are not working on any draft legislation. As time goes on, if it appears necessary or desirable, we would make such a request of the Congress.

Senator KENNEDY. Okay.

Mr. MARONEY. Now, I had indicated that I thought the difficult issue had been laid to rest by the Supreme Court decision, many of the difficult issues. In such cases, under the law as it stands, the Government must seek prior judicial approval before intercepting wire or oral communications.

The Court's opinion in the *Keith* case would, however, suggest the possibility that Congress might desire to legislate standards and procedures for court-approved electronic surveillance in domestic security cases under standards somewhat different from the standards now applicable in ordinary criminal cases. However, as was stated last week by the President, the executive branch has no present intention of seeking such amendatory legislation with respect to the area governed by the *Keith* decision. In the event that future experience demonstartes a legal void, it will then be an appropriate time to consider the necessity or desirability of requesting appropriate legislation.

[The full text of the President's remarks on this subject at his June 22, 1972 press conference follows:]

Q. Two questions about recent Supreme Court decisions, if I may ask them as two questions, because I am asking in both cases if you have any plans for meeting the situation.

In the first case, the Supreme Court rules your wiretapping program unconstitutional, saying that in cases of domestic security, wires could not be tapped without a court order. So my first question is whether you have any plans to ask Congress for legislation to restore that authority in the form of an amendment to the Safe Streets Act or other legislation.

In the second case, the Supreme Court left it up to Congress whether organized baseball came under the antitrust laws. This being a matter of some national interest, I think, I wonder if you have any plans to ask for legislation to clarify the status of organized baseball.

The PRESIDENT. On the first question, I think it is appropriate to point out that the wiretapping in cases of civilian activity, domestic civilian activity, is not, as you have described it, just this Administration's policy. As you know, this type of activity of surveillance has been undertaken, to my knowledge, going back to World War II. It reached its high point in 1963 when there were over 100 cases, as Mr. Hoover testified, in which there were taps used in cases involving domestic security.

Since that time the number of taps has gone down. It went down during the Johnson Administration, and it has sharply been decreased during the 3½ years that this Administration has been in office.

Now, as far as the Supreme Court's decision is concerned, I see no need to ask for legislation to obtain the authority, because the Supreme Court's decision allows the Government, in a case that it believes necessary, to go to a court and get a court order for wiretapping. It simply prohibits wiretapping unless there is a court order. So we will abide by that.

I should also point out that the Supreme Court's decision does not rule out wiretapping in the United States in domestic matters where there is a clear connection between the activity that is under surveillance and a foreign government. That, of course, allows us to move in the internal security area where there is a clear connection between the two. So we will, of sourse, abide by the Supreme Court's decision in this instance, and I see no need to ask for additional authority from the Congress.

Senator KENNEDY. Does this mean that the executive branch will be getting intelligence warrants without statutory authorization?

Mr. MARONEY. In wholly domestic security situations? No, sir.

Senator KENNEDY. What will you use? Do you have to use either title III or———

Mr. MARONEY. You have to use either title III or nothing.

It is important to recall, however——

Senator KENNEDY. What percent of your cases fall within title III? The statute was obviously drafted for crime detection tapping. But there must have been a number of types which you considered to be of importance for intelligence purposes that do not necessarily fall within those provisions of title III. Do you feel restricted in your attempt to gather intelligence information without some statutory authority to do so?

Mr. MARONEY. Well, of course, in most of our cases, most of the cases that the Division handles are ordinary criminal cases, the volume. In other situations, for example, espionage or sabotage, title III provides an avenue for us to get a warrant in an appropriate situation. The Attorney General-authorized electronic surveillance has been utilized, as you know, for intelligence gathering and not to secure evidence to use in a criminal case.

It is important to recall, however, that Justice Powelll, speaking for the majority, made clear that "instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country." Slip opinion, page 10. Subsequently at page 23, the Court pointed out:

As stated at the outset, this case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to the issues which may be involved with respect to activities of foreign powers or their agents.

The *Keith* decision made it clear that the Court was limiting the scope of the decision to "domestic organnization[s]. . . .composed of citizens of the United States and which ha[ve] no significant connection with a foreign power, its agents or agencies."

Senator KENNEDY. Of course, the decision did not say that warrantless foreign-intelligence taps are legal, though, did it?

Mr. MARONEY. No, it did not hold that warrantless taps on foreign agencies are legal, but the decision did not preclude the legality of such taps.

Senator KENNEDY. So that is really an open question, is it not?

Mr. MARONEY. It is an open question, not yet decided by the Supreme Court, and I think specifically carved out by the Court in this decision as well as the prior decision.

Senator KENNEDY. Of course, it would seem that a lot of the arguments which the Justice Department used in support of its position in domestic security cases could also be made with respect to your position on foreign intelligence, and yet many of those arguments were rejected in the *Keith* case. For instance, there was the argument about secrecy and your ability to convince judicial officials of the sensitive nature of various materials. that was just one of the arguments that was rejected. I was just wondering whether that has affected your thinking about the legitimacy of those kinds of arguments in the foreign field.

Mr. MARONEY. Well, I think in the foreign area, when you get into the area of foreign intelligence, the Court has recognized, I think, the President's constitutional authority in the conduct of foreign affairs to protect the Nation from attack. I think you undoubtedly have a great number more subleties of information that become involved in a determination as to whether or not a particular installation is necessary. I think the arguments that we made in the *Keith* case with respect to that are as applicable to the foreign area. I think the Court may give a different weight to those arguments in such a situation because there are not presently competing first amendment rights that the Court found quite heavy in the *Keith* case.

Senator KENNEDY. Of course in the *Pentagon Papers* case, the Justice Department felt comfortable in making sensitive material available to judges. The Department had sufficient confidence in the judges in that case to be willing to make this kind of material available to the courts.

Mr. MARONEY. Well, of course, we have made sensitive material available in a large number of cases.

Senator KENNEDY. Sure.

Mr. MARONEY. In the *Keith* case, itself, for example, information which we thought was sensitive and still think is.

Senator KENNEDY. So the argument which is often made—about unwillingness to get court orders on foreign intelligence taps because it would mean you would have to make sensitive material available to courts—that argument really has very little standing in your own view?

Mr. MARONEY. No, I do not think it has little standing. I think it is axiomatic that the more distribution you give to secrets, the less secrecy you have. It is certainly more desirable if you have sensitive information if you are able to restrict it in the closest possible way.

The Court recognizes that it may be difficult to distinguish between domestic and foreign unlawful activities directed against the Government of the United States where there is collaboration in varying degrees between domestic groups and organizations and agents or agencies of a foreign power. The committee has asked that we address ourselves to the question of what level of foreign dominance and control of a domestic group would be considered sufficient to bring the group into the area of foreign activities which the Court has not yet ruled upon.

The *Keith* decision has suggested a standard of significant connection with a foreign power, its agents or agencies. We do not interpret this as meaning casual, unrelated contacts and communications with foreign governments or agencies thereof. We would not try to apply this standard without the presence of such factors as substantial financing, control by or active collaboration with a foreign government and agencies thereof in unlawful activities directed against the Government of the United States. Obviously, such factors will be present in a very minimum number of situations.

I wish to assure the committee on behalf of the Attorney General, that the Department of Justice accepts both the letter and the spirit of the Court's ruling in the *Keith* case.

Senator KENNEDY. What do you think the spirit of the Court's ruling in the *Keith* case is?

Mr. MARONEY. Well, I think the spirit of the case is that where you are dealing with wholly domestic organizations that may bring into play first amendment considerations, the first amendment considerations outweigh the governmental necessity in securing warrantless electronic surveillance and require that the Government follow the provisions of title III in the Court-authorized warrant.

Senator KENNEDY. The decision contained, I thought, a strong and eloquent plea about the importance of the convergence of first and fourth amendment values:

> National security cases, moreover, often reflect a convergence of first and fourth amendment values not present in cases of ordinary crime. Though the investigative duty of the executive may be stronger in such cases, so also is their greater jeopardy to constitutionally protected speech. . . . Fourth amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect domestic security. Given the difficulty of defining the domestic security interest the danger of abuse in acting to protect that interest becomes apparent. . . . The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.

There seems to be a strong commitment here to the convergence of first and fourth amendment rights. I was just wondering if you shared that view and——

Mr. MARONEY. Yes, sir.

Senator KENNEDY. You were impressed by its discussion in the opinion.

Mr. MARONEY. Yes, sir; very definitely.

It is the intention of the executive branch to utilize electronic surveillance in present and future national security matters in full and ungrudging application of the rationale of the decision.

In connection with the latter point, I think it appropriate to note that it was the Department of Justice which sought a definitive resolution of the difficult constitutional questions presented by the *Keith* decision at the earliest possible time. When the district court ruled against the Government's position in this case, we had no right of appeal under the law as it then stood. We therefore resorted to the unusual remedy of petitioning the court of appeals for the extraordinary writ of mandamus on the basis that the question was of substantial public importance which should be decided by the courts. It was as a result of that effort, that the matter has now been decided, which is better for everyone concerned.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Maroney follows:]

STATEMENT BY KEVIN T. MARONEY, DEPUTY ASSISTANT ATTORNEY GENERAL, INTERNAL SECURITY DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. Chairman and Members of the Subcommittee, I am happy to appear here today on behalf of the Department of Justice in response to your request for our views on the subject of electronic surveillance and in particular, concerning the impact of the Supreme Court's decision last week in the case of *United States* v. *United States District Court for the Eastern District of Michigan* No. 70–153 decided June 19, 1972 and more popularly known as the *Keith* case.

The immediate impact of the *Keith* case was set forth clearly by Attorney General Richard G. Kleindienst in his statement of June 19, 1972. Let me quote:

"In accordance with the decision of the Supreme Court, I have today directed the termination of all electronic surveillance in cases involving domestic security that conflict with the Court's opinion. Hereafter, surveillance will be undertaken in domestic security cases only under procedures that comply with the Court's opinion."

Whatever problems, Mr. Chairman, some may have had with respect to the difficult issue of electronic surveillance involving wholly domestic organizations have, in great part, been laid to rest by the Supreme Court decision. In such cases, under the law as it stands, the Government must seek prior judicial approval before intercepting wire or oral communications.

The Court's opinion in the *Keith* case would, however, suggest the possibility that Congress might desire to legislate standards and procedures for court approved electronic surveillance in domestic security cases under standards somewhat different from the standards now applicable in ordinary criminal cases. However, as was stated last week by the President, the Executive Branch has no present intention of seeking such amendatory legislation with respect to the area governed by the *Keith* decision. In the event that future experience demonstrates a legal void, it will then be an appropriate time to consider the necessity or desirability of requesting appropriate legislation.

It is important to recall, however, that Justice Powell, speaking for the majority, made clear that "the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country." Slip opinion, page 10. Subsequently at page 23, the Court pointed out:

"As stated at the outset, this case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the

issues which may be involved with respect to activities of foreign powers or their agents."

The *Keith* decision made it clear that the court was limiting the scope of the decision to "domestic organization[s] . . . composed of citizens of the United States and which ha[ve] no significant connection with a foreign power, its agents or agencies." The Court recognized that it may "be difficult to distinguish between domestic and foreign" unlawful activities directed against the Government of the United States where there is collaboration in varying degrees between domestic groups and organizations and agents or agencies of a foreign power." The Committee has asked that we address ourselves to the question of what level of foreign dominance and control of a domestic group would be considered sufficient to bring the group into the area of foreign activities which the Court has not yet ruled upon.

The *Keith* decision has suggested a standard of "significant connection with a foreign power, its agents or agencies." We do not interpret this as meaning casual, unrelated contacts and communications with foreign governments or agencies thereof. We would not try to apply this standard without the presence of such factors as substantial financing, control by or active collaboration with a foreign government and agencies thereof in unlawful activities directed against the Government of the United States. Obviously, such factors will be present in a very minimum number of situations.

I wish to assure the Committee on behalf of the Attorney General, that the Department of Justice accepts both the letter and the spirit of the Court's ruling in the *Keith* case. It is the intention of the Executive Branch to utilize electronic surveillance in present and future national security matters in full and ungrudging application of the rationale of the decision.

In connection with the latter point, I think it appropriate to note that it was the Department of Justice which sought a definitive resolution of the difficult constitutional questions presented by the *Keith* decision at the earliest possible time. When the District Court ruled against the Government's position in this case, we had no right of appeal under the law as it then stood. We therefore resorted to the unusual remedy of petitioning the Court of Appeals for the extraordinary writ of mandamus on the basis that the question was of substantial public importance which should be decided by the courts. It was as a result of that effort, that the matter has now been decided, which is better for every one concerned.

Senator KENNEDY. You talk about this unusual remedy of petitioning the court of appeals. What other choice did you really have?

Mr. MARONEY. Well, the choice that we had was disclosure of the information to the defendant.

Senator KENNEDY. Or dismissal?

Mr. MARONEY. Or suffering the dismissal of the case.

Senator KENNEDY. So it was really to carry through your own interest in maintaining a successful prosecution, rather than, should we say, the goodness of your heart?

Mr. MARONEY. I did not say out of the goodness of our heart. I indicated that we were as aware as anyone else that this was a constitutional problem hanging over all of us. We were aware of the difficulties of the legal problems involved and we were as anxious as anyone else to have the matter settled.

Senator KENNEDY. After hearing your statement here this morning, and after seeing Mr. Kleindienst's statement on June 19 and the President's comments at his news conference on June 22, I found it somewhat troubling that nothing has been said by the Justice Department or the President about what you are going to do to cleanse all the Government files of the information that came from conversations which were tapped or bugged unconstitutionally. Could you tell us what your plans are about that?

Mr. MARONEY. I know of no such plans. Obviously, I do not think we could very well destroy the information. In the event of a future criminal proceeding in which a defendant may have been overheard on one of these, we would be obligated to produce to the court and to the defendant, under a protective order, any logs of overhearings of his conversations.

Senator KENNEDY. So the reason, then, is for the preservation of the defendant's rights?

Mr. MARONEY. Well, I think we have to do that; otherwise, we would have no way of determining any possible *Keith* issue in a future situation.

Senator KENNEDY. Is that the only basis of access to those files?

Mr. MARONEY. The only basis of access?

Senator KENNEDY. Yes, only when the defendant raises these questions?

Mr. MARONEY. Yes, sir.

Senator KENNEDY. There is no other basis for access to them?

Mr. MARONEY. No, sir.

Senator KENNEDY. Of course the Army agreed last year to destroy some of the things contained in their files from spying on civilians. There was a letter from the Defense Department's General Counsel to Senator Ervin on June 10, 1971, which said, "The civil disturbance information in CRIS"—that is the Counterintelligence Records Information System—"was stored on four magnetic tapes and discs. They were all destroyed on April 12, 1970, by degaussing, for example, the information was removed from the discs and tapes by passing them through a magnetic field. No other discs or tapes contained the information which was in the Fort Monroe program. Supporting files consisted of boxes of IBM cards, existing printouts, and the user manuals. These related files were destroyed on April 22, 1970." This letter also said, "To comply with the spirit of the new DA [Department of the Army] policy, however, all dossiers are reviewed for unauthorized materiel—which is removed and destroyed—before being released to the requester."

[The complete text of the June 10, 1971 letter to Senator Ervin from the General Counsel, Department of Defense, follows:]

GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE,
Washington, D.C., June 10, 1971.

Hon. SAM J. ERVIN, Jr.,
Chairman, Subcommittee on Constitutional Rights, Committee on the Judiciary, U.S. Senate, Washington, D.C.

DEAR MR. CHAIRMAN: Your questions concerning the Fort Monroe and Fort Hood data banks and the additional files referred to on page 3 of your March 30, 1971 letter to Secretary Laird have been referred to me for reply.

As you know, representatives from the Army met with the Subcommittee's Chief Counsel for several hours on April 15 to respond to the six questions set forth on page 2 of your letter. During these discussions, he raised additional questions about the Fort Monroe and the Fort Holabird computer systems. Answers to these questions are enclosed at Tab A.

It is believed that the submissions included with this letter, plus certain follow-up actions by the Department of the Army, will provide the Committee with as complete a report of the computer operations as possible under the circumstances. In this respect, it is noted that the draft report of the Constitutional Rights Subcommittee Staff, dated April 26, 1971, suggests a certain unresponsiveness on the part of the Department of the Army. The record is to

the contrary. The Department has endeavored at all times to furnish a full and complete account despite the fact that the computer operations in question have long since been disbanded, and the computer print-outs at Fort Holabird and Fort Monroe destroyed except for those which are now in the temporary custody of the Subcommittee. To secure a technical explanation, the Department of the Army contacted the originators of the computer system and obtained their recollections as to the meaning of the computer code symbols.

With reference to your request for further information on the Fort Monroe and Fort Hood computer data banks, answers to your various questions have been prepared from the information presently available and from the recollection of those who worked on these programs. The destruction of these computer data banks and related files last year makes it quite difficult to answer many of your questions. In this regard, the Army is unable to provide you copies of any documents, manuals, or other publications relating to the establishment of these systems because they are no longer available and in some cases existed only in a fragmentary and informal form. However, two pamphlets on coding instructions for the Fort Holabird computer are being held by the Department of Justice for purposes of the *Tatum* v. *Laird* litigation. These may be of interest to you in your inquiry.

The Fort Monroe computer data bank, known as the Counterintelligence Records Information System (CRIS), was established in January 1968 but was not computerized until May 1968, CONARC sought and obtained approval for the computerization of this sytem in April–May 1968 in accordance with the provisions of paragraph 2–1, Army Regulation 18–2 (attached). This regulation does not establish the criteria for reviewing the propriety of a particular system; it only outlines the procedures for reviewing the feasibility of a particular program in light of available and prospective computer resources and requirements. On April 1, 1970, the Secretary of the Army issued a policy letter which required his personal approval of any computerized data bank on civilians not affiliated with the Department of Defense and only after consultation with Congress. DoD Directive 5200.27 now imposes the requirement that the Chairman of the Defense Investigative Review Council approve such computer operations.

CRIS, the Fort Monroe system, was designed to retrieve civil disturbance information rapidly and generate data and statistics to assist CONARC in the prediction of civil disturbances which might result in the deployment or commitment of federal troops. The attempt to predict possible civil disturbances or incidents related directly to the requirements placed on CONARC to provide Task Forces for deployment and for actual use in civil disturbances in accordance with the Army Civil Disturbance Plan (Garden Plot). The statistics and other data produced by this program were considered to be a necessary adjunct to the requirements and responsibilities imposed by the Army Civil Disturbance Plan, and it was hoped that this data would assisst the CONARC federal troops.

The Cris contained three basic categories of information with a cross-reference retrieval capability among them: personalities, organizations, and incidents. The information itself was stored on magnetic discs, with a backup file on magnetic tape. Information for CRIS was received from USAINTC, CONUSAMDW, and the FBI. There was not, however, a direct interconnection between other computers nor was the information fed directly into CRIS over teletype or other electrical means. Recipients of the information produced by CRIS included: Office Deputy Chief of Staff for Intelligence, CONARC; the Deputy Chiefs of Staff for Intelligence, CONUS Armies and Military District of Washington; HQ, USAINTC; Assistant Chief of Staff for Intelligence, DA; and the Commander, Military Traffic Management and Terminal Service. There is no way of determining how many printouts or other information derived from CRIS were produced and forwarded to the recipients listed above. However, the June 9, 1970 Army policy letter required the destruction of all civil disturbance information on civilians.

It should be pointed out that only 2.5% of available computer time was used on CRIS. The remaining computer time was consumed by 8 major programs, all of which dealt directly with CONARC's command and control functions. These programs were: Force Status, Unit Identification, Automated Army Unit Readiness Reporting System, Contingency Planning Troop List, CONARC movement Planning and Status, Computerized Airlift Planning, and Contingency Plan Map System.

The civil disturbance information in CRIS was stored on four magnetic tapes and discs. They were all destroyed on April 12, 1970, by degaussing, i.e., the information was removed from the discs and tapes by passing them through a magnetic field. No other discs or tapes contained the information which was in the Fort Monroe program. Supporting files consisted of boxes of IBM cards, existing printouts, and the user manuals. These related files were destroyed on April 22, 1970.

You have asked whether a civilian approved the initiation of the Fort Monroe program. The requirement for the approval of such computer data banks was not imposed until April 1, 1970, and, hence, there was no requirement for such approval at the time the system was initiated. The Office of the Army General Counsel did become aware of the system on or about March 1, 1970. I would stress that there was no effort to hide the system in question; it was discussed and explained at various briefings to high military officials and was viewed as a normal adjunct to the Army's civil disturbance program.

The Fort Hood system, the second system referred to in your letter, did not reach the same stage of development as CRIS. In fact, it did not become fully operational before its destruction on August 15, 1970. By way of background, a feasibility study was begun in July 1969 at Fort Hood on a computer program which could provide III Corps with the ability to retrieve civil disturbance information rapidly and assist it in predicting disturbances within its geographical area of responsibility. Under the Army Civil Disturbance Plan (Garden Plot), Fort Hood was required to provide three civil disturbance task force headquarters and six civil disturbance brigades for possible deployment in a civil disturbance situation. The computerization of the data contained at Fort Hood was intended to supply the intelligence required to respond efficiently and rapidly to a civil disturbance situation.

The program was run on a computer which was used primarily in the areas of supply, finance, accounting, and maintenance with the secondary purpose of providing support for various systems development such as the Division Logistic Systems Tests and currently the Combat Service Support System. In fact, only 0.008 of 1 percent of computer time was used in the formulation of the civil disturbance program. A request for program approval was not submitted under the provisions of paragraph 2–1, AR 18–2, described above. However, since AR 18–2 relates only to the feasibility of the system, the question of the propriety of implementing such a system would not have been reviewed under AR 18–2. Of course, new policy letters and directives now impose a requirement that such a computer data bank be approved by civilian officials.

The information for the data banks was received from the FBI, USAINTC, and from liaison contacts with local authorities. The data bank itself listed in alphabetical order various civilian organizations which were deemed to have some relation to the III Corps responsibility under Garden Plot. Under the listed organizations, the names of certain members of the organization were also included. Since this system did not reach full operational status, only two copies of a printout were produced for distribution outside of Fort Hood. The Deputy Chief of Staff Intelligence, 4th U.S. Army, received one copy which was subsequently destroyed in August 1970. One was also forwarded to the Assistant Chief of Staff for Intelligence, DA.

The computer program at Fort Hood was not known at DA, Headquarters until the latter part of April 1970 when an exception was sought from the provisions of the April 1, 1970 letter requiring the destruction of computerized data banks on civilians not affiliated with the Department of Defense. To review the propriety of the exception, ACSI, DA, requested a copy of the printout from the Fort Hood computer. This copy (referred to above) was forwarded, and after review of the document, the exception was denied and the data bank was ordered destroyed on August 5, 1970. The data bank and computer program on magnetic tape (there were no discs) were then destroyed on August 15, 1970.

As indicated above, the printout, from the Fort Hood system sent to the 4th U.S. Army was previously destroyed. It was thought that the printout provided to ACSI, DA, the only other printout, had also been destroyed. Although there had never been any written record of destruction to confirm this, several prior searches had failed to discover the document in question. However, on May 11, 1971, the last remaining printout from Fort Hood was discovered by accident among some files in the Office of the Assistant Chief of Staff for

Intelligence, Department of the Army. On May 21, 1971, the Acting General Counsel of the Army wrote to the Department of Justice requesting its advice on the proper disposition of this item in view of the *Tatum* v. *Laird* litigation. The Justice Department has advised the Department that it should be retained for litigation purposes.

You asked about the existence of a set of records called the "Van Deman" files. Major General Ralph Van Deman, who formerly headed Army Intelligence, compiled intelligence files during the period of 1929–1952. There is no indication, however, that he collected these files prior to his retirement in 1929.

The files, for the most part, consisted of four general categories: (1) collection of various newspapers from the West Coast alleged to be communist or communist-affiliated; (2) literature and reference material on or produced by alleged communists; (3) a photo album of assorted individuals: and (4) files on individuals and organizations based upon information acquired from various agencies and private sources. The information in the latter category largely dealt with communist activities.

The Assistant Chief of Staff for Intelligence, Sixth Army, assumed custody of at least some of General Van Deman's files on January 22, 1952. It is believed that certain portions of the files were removed by associates of General Van Deman before the Sixth Army acquired these files, but this cannot be verified. The reasons for assuming custody is not entirely clear. It is quite possible that there was some informal arrangement between the Assistant Chief of Staff for Intelligence, Sixth Army, and General Van Deman for the transfer of these items at General Van Deman's death.

The files in the possession of the Sixth Army were shipped in 1958 to what is now designated as the United States Army Investigation Records Repository (USAIRR). Following this transfer, the index cards prepared by General Van Deman for use with his material were replaced by punch cards and integrated into the USAIRR index. His own index cards were then destroyed. In 1968, the punch cards prepared from the earlier index cards were also destroyed, and all reference to these materials in the Defense Central Index of Investigations was thereby deleted. The Van Deman files were then segregated within the USAIRR. After 1968, these files were not referenced by the DCII.

These files remained in the USAIRR, although segregated, until March 2, 1971 when they were transferred to the Internal Security Subcommittee of the Senate Judiciary Committee pursuant to a written request by the Chairman of the Judiciary Committee. We have found no record of an inquiry to Mr. Froehlke or to the Department of Defense related directly or indirectly to the Van Deman files prior to your letter of March 30.

In regard to your last series of questions on page 3 of your letter, the Army implemented a policy in February 1971 of reviewing each file at the USAIRR prior to its release to an authorized official for the purpose of removing material which cannot be retained under our present directives. Mr. Froehlke explicitly informed you of this policy in his appearance.

"There are dossiers within the Army Investigative Records Repository which contain FBI reports and other material which do not meet current Army criteria for retention. A mass screening of the 8 million dossiers would be a long and very expensive undertaking. To comply with the spirit of the new DA policy, however, all dossiers are reviewed for unauthorized material—which is removed and destroyed—before being released to the requester. (Report of Proceedings held before the Subcommittee on Constitutional Rights of the Committee on the Judiciary Mar. 2, 1971, Vol. 4, p. 600.)"

Files have been and will continue to be screened in accordance with this policy for the purpose of removing and destroying material not authorized for retention under current policy. Generally speaking, there has been no special effort to segregate files to be screened. However, upon discovering that files on certain prominent individuals contained information which is no longer authorized to be retained, the Army has specifically screened out this material.

I trust that this information will assist you in your inquiry.

Sincerely.

J. FRED BUZHARDT.

Are you planning any similar procedure at the Justice Department?

Mr. MARONEY. No, sir.

Senator KENNEDY. Do you think there should be such a procedure? I do not know whether anyone at the Justice Department has had a chance to think about this problem. Perhaps you could write us a note about what you are doing, or about what you will do, or about why you will not do it if that is what you decide. Or are you prepared to say something about that right now?

Mr. MARONEY. I think as I indicated, if we were to follow that procedure, we would have a substantial legal problem on the question of taint in a future criminal case. The only way we can demonstrate in such a case that none of the evidence being used in the case has been tainted is to turn over the logs, have a hearing, and then demonstrate that none of the evidence being used at the trial resulted from the electronic surveillance.

Senator KENNEDY. Where is the material now that came from the illegal taps? Is it in one place, or is it still at different agencies? Have you collected it from the other agencies? Have you issued any regulations, for example, that none of this material will be available to anyone unless there is a specific order from the Attorney General and that then it will only be for the purposes of protecting a defendant's rights? Has anything been done about that?

Mr. MARONEY. No, sir.

Senator KENNEDY. Well, should there not be? Suppose there is some of that material in other departments. For example, how will they know over at the Defense Department what you are saying up here? Has the Attorney General done anything about that? Should he do something about it? Are you not concerned that something should be done to try to achieve what you have outlined here—that is that this information not be generally available?

Mr. MARONEY. None of this information is generally available, Senator.

Senator KENNEDY. Well, not generally available to the public, but——

Mr. MARONEY. All of it is handled as confidential investigative material. It has a limited dissemination. I do not think there is any danger of any improper use of this information.

Senator KENNEDY. Well, of course, even though there may be some procedures about dissemination of investigative information, it is still in the files. I am not so sure that it should be left in those same investigative files and available even to the people who are entitled to obtain investigative files. Why can't it just be assembled and put into a separate place, under a specific restriction—only for protecting defendants' rights.

Mr. MARONEY. Well, of course, the logs themselves are maintained by the FBI. They are not disseminated in any place. As a matter of fact, the only time there is an examination of those logs by anybody other than the people in the FBI is in connection with a pending court procedure in which a question arises as to turning logs over to a dependant or the court for in camera inspection.

Senator KENNEDY. Of course the original purpose of getting the information was to use it.

Mr. MARONEY. And some of the investigative information would be in investigative files, some pieces of the information.

Senator KENNEDY. How do you get it out of those files?

Mr. MARONEY. How do you get it out?

Senator KENNEDY. Yes, how do you get it out so that it just is not available in the files for anyone—even those with access—to review it?

Mr. MARONEY. Well, it would be a difficult job to go back and——

Senator KENNEDY. Well, the Army did it.

Mr. MARONEY. Well, the Army essentially just destroyed all of its files in that area.

Senator KENNEDY. But you are not even able to——

Mr. MARONEY. It did not just destroy 10 percent or 1 percent of the information in those files.

Senator KENNEDY. Well, we do not really know how difficult it would be because no one has tried to do it.

Mr. MARONEY. Well, no one has tried to do it and I have no doubt that it would be an extremely difficult job.

Senator KENNEDY. Is that because there is so much of it?

Mr. MARONEY. No, I think because you would have to cull maybe, you know, one-thousandth of a percent out of a number of files.

Senator KENNEDY. Could you tell us how many devices were turned off as a result of the *Keith* opinion?

Mr. MARONEY. There were six removed as a result of the *Keith* decision, leaving a total of 27.

Senator KENNEDY. Six devices, or organizations, or what?

Mr. MARONEY. Telephone wire taps and microphone installations.

Senator KENNEDY. And the decisions to turn those off were all made by the Attorney General in consultation with you?

Mr. MARONEY. Yes, sir.

Senator KENNEDY. Were those surveillances of organizations or individuals? Can you tell us?

Mr. MARONEY. Some of each.

Senator KENNEDY. If you had a number of devices on one organization, would that be counted as one device, or several?

Mr. MARONEY. Each installation, each device is counted as one installation.

Senator KENNEDY. Can you give us any idea of how long those devices had been in operation?

Mr. MARONEY. I do not have any figures on that, Mr. Chairman.

Senator KENNEDY. Could you provide it for use if you have time?

Mr. MARONEY. I will try to provide it; yes, sir.

[Subsequent to the hearing, Deputy Assistant Attorney General Maroney submitted a letter to the subcommittee dated August 2, 1972, containing the following answer to Senator Kennedy's question:]

* * * * * * *

On page 29 of the reporter's transcript of the hearing on that date, you made a request for information on the length of operation of the six electronic surveillances in the national security field which were discontinued by the FBI as a result of the United States Supreme Court decision of June 19, 1972, in the *Keith* case. One of these electronic surveillances was operated for 21 months; two for 18 months; one for 4½ months; one for 3 months; and one for 2 weeks.

Of course, in accordance with established practice, those of the aforementioned surveillances which were in operation more than 3 months were reviewed and reauthorized every 3 months by the Attorney General.

* * * * * * *

(The full text of the above letter is reprinted at page 47.)

Senator KENNEDY. There was a report in the June 24 edition of the *Cape Cod Standard-Times* quoting Mr. Kleindienst as saying that the Department "had canceled some 10 wiretaps"——

Mr. MARONEY. I think he said less than 10. He was not giving precise figures.

Senator KENNEDY. I am not trying to catch you.

Mr. MARONEY. But these figures are the precise figures.

Senator KENNEDY. Can you tell us how many national security taps or bugs are still being operated?

Mr. MARONEY. Twenty-seven.

Senator KENNEDY. Again, are those different groups or targets or are those the total number of devices? Do you know what I am driving at? If there is an organization on which you have more than one device is that counted as one or is that several?

Mr. MARONEY. If there were two devices——

Senator Kennedy. If you have one organization and it is tapped five times, is that considered one or five?

Mr. MARONEY. Five.

[Subsequent to the hearings, the subcommittee received a letter from Deputy Assistant Attorney General Maroney, dated August 2, 1972, containing the following clarification:]

* * * * * * *

On pages 29 and 30 of the reporter's transcript there was a brief colloquy as to the method of computation of electronic surveillances, that is, when we say there are 27 electronic surveillances in effect on a given date does that represent "targets" or the number of devices. I am advised by the FBI that the number of surveillances indicated represent premises of organizations or individuals without regard to the number of instruments which may be involved in effectuating the surveillances.

* * * * * * *

[The full text of the above letter is reprinted at page 47:]

Senator KENNEDY. Could you give us a breakdown by the five statutory categories, such as clear and present danger, threat of overthrow, and foreign intelligence information?

Mr. MARONEY. Well, I have not had time to break that out. Most—practically all—of those would be foreign intelligence, strictly foreign intelligence.

Senator KENNEDY. If most are for foreign intelligence, what are the remaining ones for?

Mr. MARONEY. Well, what we have been doing in the past 6 months to a year is when the Attorney General authorizes one of these installations, he makes precise findings in terms of the five criteria set forth in 2511(3). I have not had a chance this week to make that breakdown; I think we could do that for you and I think it would go back where we would have that capability for 6 months to a year.

Senator KENNEDY. Could you do that for us?

Mr. MARONEY. Yes, sir.

Senator Kennedy. That would be helpful.

[Subsequently to the hearing, Deputy Assistant Attorney General Maroney submitted a letter to the subcommittee, dated August 2, 1972, containing the following information:]

* * * * * * *

On page 30 of the reporter's transcript, you requested a breakdown of the statutory categories under Title 18, U.S. Code, Section 2511.3, used by the Attorney General in authorization of the 27 electronic surveillances operated by the FBI as of June 29, 1972. Set forth below are the statutory categories and the number of times each category was used in the Attorney General's authorization of these 27 electronic surveillances. It should be noted that many of the authorizations were based on more than one statutory category.

Category:	*Electronic surveillances authorized under category*
Category 1—To protect the Nation against actual or potential attack or other hostile acts of a foreign power	2
Category 2—To obtain foreign intelligence information deemed essential to the security of the United States	23
Category 3—To protect national security information against foreign intelligence activity	15
Category 4—To protect the United States against the overthrow of the Government by force or other unlawful means	1
Category 5—Or against any other clear and present danger to the structure or existence of the Government	1

* * * * * * *

(The full text of the above letter is reprinted at page 47.)

Is there any possibility that some more of these will be turned off as a result of the Supreme Court opinion?

Mr. MARONEY. Well, no, sir; a determination was made with respect to these, that they are all appropriate in terms of the *Keith* decision.

Senator KENNEDY. Could you tell us how many are left on domestic groups?

Mr. MARONEY. There are none on wholly domestic organizations in terms of the definition used in the *Keith* opinion.

Senator KENNEDY. But evidently some on domestic groups that have some foreign activity?

Mr. MARONEY. Foreign connections. But as I indicated in my opening statement, that number is a very, very minimal number.

Senator KENNEDY. Is the Department of Justice taking the position that the *Keith* opinion authorizes electronic surveillance without a warrant where activities of foreign powers are concerned?

Mr. MARONEY. That it authorizes? Our position is that the *Keith* decision left that undecided.

Senator KENNEDY. So you are going to continue to do it without warrant?

Mr. MARONEY. In this particular area; yes, sir.

Senator KENNEDY. What do you believe your authority to be for that?

Mr. MARONEY. The presidential authority that we relied on in the *Keith* case. We argued in the *Keith* case both the presidential authority in the area of foreign intelligence and with regard to domestic organizations aiming at overthrow of our constitutional system. The court dealt only with the wholly domestic organizations and left open the foreign intelligence area.

Senator KENNEDY. Does that come under an inherent power doctrine?

Mr. MARONEY. The constitutional authority of the President in the field of foreign affairs as well as to protect the Nation against attack.

Senator KENNEDY. We are going to recess very briefly and will be right back.

[Recess]

Senator KENNEDY. The subcommittee will come to order.

As I understand it, there has been the removal of only some six taps since the *Keith* decision, is that correct?

Mr. MARONEY. Yes, sir.

Senator KENNEDY. Do you have any intention of trying to reinstall any of those six either under title III or any other statute?

Mr. MARONEY. None that I know of at the present time; no, sir.

Senator Kennedy. Well, you would know about it if it was being thought about, would you not?

Mr. MARONEY. Well, I would think so. I have not heard of anyone suggesting it.

Senator KENNEDY. Were any not taken off and just switched over to a title III authorization?

Mr. MARONEY. You mean converted to title III?

Senator KENNEDY. Converted.

Mr. MARONEY. No, sir; of these six.

Senator KENNEDY. Can you tell us how many of the other 27—is it 27?

Mr. MARONEY. Twenty-seven; yes, sir.

Senator Kennedy. How many of those will be converted to title III?

Mr. MARONEY. I do not think any of them will be.

Senator KENNEDY. And how many of those 27 are domestic organizations?

Mr. MARONEY. It is an extremely minimal number.

Senator KENNEDY. Can you say less than three?

Mr. MARONEY. Less than three; yes, sir.

Senator KENNEDY. I have two more guesses. Less than two?

Is it difficult for you to answer whether it is one or two?

Mr. MARONEY. I do not—it is my understanding from the Attorney General that it is less than three. Now, I do not know that I could give you any answer whether it is one or two.

Senator KENNEDY. Do you believe that the Court intended the phrase "no significant connection with a foreign power, its agents or agencies" to be a dividing line between a clearly domestic area and a gray area, or do you think that the phrase is the dividing line between the domestic area and the foreign area?

Mr. MARONEY. Well, I think it depends on two things: One, what the organization may be trying to accomplish, and second, the presence of significant foreign connections. I think both those things have to be taken into consideration.

Senator KENNEDY. Would you agree that that there can be domestic groups with some significant foreign connection which still retain their primarily domestic character for purposes of the first and fourth amendments?

Mr. MARONEY. Well, yes; I do think so.

Senator KENNEDYS. Have you issued any directives or memoranda containing your interpretation of where the dividing line is, or how you will decide which groups are on the foreign side of the line?

Mr. MARONEY. No, sir; other than that, as I tried to indicate in the opening statement, and as I previously indicated, all these deter-

minations are made personally by the Attorney General. He will make them in light of the fact situation at present and in the light of the court decision in *Keith*.

Senator KENNEDY. How will anyone in the government know what is permissible unless you come up with some standards, guidelines, and interpretations?

Mr. MARONEY. Because the Attorney General has to authorize each and every one of these.

Senator KENNEDY. But how will a person out in the field know whether it is even worth asking for authorization, if he is not getting some guidelines as to what is legitimate and what is not?

Mr. MARONEY. Well, more definitive guidelines may be laid down in the future. As of now, we have not had an opportunity to formulate any guidelines other than the reliance on the *Keith* case and the interpretation that I have tried to place on that particular part of it.

Senator KENNEDY. Has the FBI issued any guidelines to its agents, for example, to give them a yardstick to decide whether they should request authorization for taps?

Mr. MARONEY. Well, I do not know if—I mean they do have standing instructions and procedures. Whether they have done anything beyond bringing the *Keith* case to the attention of the people that need that information and the fact of the action of the Attorney General in directing the discontinuance in these patricular instances——

Senator KENNEDY. We would like to know whether after the *Keith* case there was any modification of any of the FBI's regulations so that they would conform to the decision? Could you find that out?

Mr. MARONEY. I would be glad to try to.

Senator KENNEDY. And if there was—or wasn't—would you let us know?

Mr. MARONEY. Yes, sir.

Senator KENNEDY. We would like to see those regulations. If there are any, I request that they be made available for our information. I would appreciate it if you would do that.

[Subsequent to the hearing, Deputy Assistant Attorney General Maroney submitted a letter to the subcommittee, dated August 2, 1972, containing the following answer in response to Senator Kennedy's request:]

* * * * * * *

The committee further requested any written guidelines which had been issued by the Department as a result of the Supreme Court's decision in the *Keith* case. In view of the fact that almost all electronic surveillances now authorized by the Attorney General will be strictly in the area of foreign intelligence, and since all requests for electronic surveillance authorizations are thoroughly screened within the Federal Bureau of Investigation and personally by the Attorney General, it is not believed necessary to promulgate any additional guidelines as a result of the *Keith* decision.

* * * * * * *

[The full text of the above letter is reprinted at page 47.]

I would like to get into the question of the dividing line between domestic and foreign. Would you spell out the degree of foreign activity which the Department of Justice is applying in deciding whether a group falls within the purview of the *Keith* case or not?

What level of foreign government financing would be a determinant? Would it be a large amount, or a large percentage? You mentioned financing, for example, in your statement. Does that mean dollar value or just percent?

Mr. MARONEY. I think that is just one factor that should be taken into consideration in connection with the overall determination. I do not think that any one factor standing alone necessarily leads you to the conclusion that it is a domestic organization with significant foreign connections.

Senator KENNEDY. Just a gift, for example. Would that be considered a foreign——

Mr. MARONEY. I suppose it would depend on the nature of the gift or the purpose of the gift. Whether it is financing of unlawful activity directed against the Government of the United States—that would be a more significant factor.

Senator KENNEDY. What if individuals, or members of a group, travel to Hanoi, for example. Does that taint the whole group?

Mr. MARONEY. No, as we indicated, that casual, unrelated contact would not be the kind, the level of connection——

Senator KENNEDY. Well how about something beyond casual. How about humanitarian reasons? There have been different religious groups which have gone over to Hanoi and brought medical supplies——

Mr. MARONEY. That would not be sufficient; no, sir.

Senator KENNEDY. There are some labor leaders who have gone over to Hanoi and had exchanges with members of the North Vietnamese Trade Union Movement.

Mr. MARONEY. Absolutely not.

Senator KENNEDY. And have also traveled to Paris and talked with the representatives of the NLF there. That type of contact would not be sufficient even though it might be significant?

Mr. MARONEY. No, sir.

Senator KENNEDY. In addition to the foreign factors the Court spoke of involvement in unlawful activities and indicated that those activities must be directed against the Government of the United States. Do you agree that the unlawful activities must also meet the tests prescribed by Congress, namely that they be in one of five categories—"necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power;" necessary "to obtain foreign intelligence information deemed essential to the security of the United States;" necessary "to protect national security information against foreign intelligence activities;" necessary "to protect the United States against the overthrow of the government by force or other unlawful means;" or necessary to protect "against any other clear and present danger to the structure or existence of our government?"

Mr. MARONEY. Yes, sir; we do agree with that.

Senator KENNEDY. That they have to fall within those categories?

Mr. MARONEY. Yes, sir.

Senator KENNEDY. Is the Department of Justice taking the position that you can go into court now and obtain a warrant to tap a purely domestic organization to get intelligence information?

Mr. MARONEY. No, sir,! I do not believe so. In such a situation, we would have to follow the provisions and requirements of title III.

Senator KENNEDY. Which does not include intelligence information?

Mr. MARONEY. No, sir.

Senator KENNEDY. And under the *Keith* decision, you would not be permitted to do so.

Mr. MARONEY. It does not permit it; no, sir.

Senator KENNEDY. So it is clear, then, that you would need to get a special warrant other than under title III; you need new legislation?

Mr. MARONEY. I think so; yes, sir.

Senator KENNEDY. Could you tell us how a national security tap originates? Is it the Attorney General's idea in the first instance, the FBI Director's idea, or some individual FBI agent's decision, or what?

Mr. MARONEY. By far, the most arise in connection with the investigative processes of the FBI, and any suggestion for the installation of an electronic surveillance device in this area is subjected to very thorough review at several levels of the FBI. It would have to be personally, of course, approved by the Director of the FBI and then would be submitted to the Attorney General after having been reviewed by the Assistant Attorney General in charge of the Internal Security Division, who would then confer with the Attorney General on the request. The Attorney General now makes findings of fact based on the request and the information set forth therein and the criteria set forth in 2511(3).

Senator KENNEDY. Well, what I am directing your attention to is the question of who reviews the requests for taps outside the FBI. What happens when these requests reach the Attorney General's desk? I had always understood that the only person in the Justice Department who examined these requests was the Attorney General.

Mr. MARONEY. The requests for installation?

Senator KENNEDY. Yes.

Mr. MARONEY. Any requests for installation go through the director of the FBI, come over to the Department, and are reviewed by the Assistant Attorney General of Internal Security and then up to the Attorney General, you get his recommendation.

Senator KENNEDY. When did that procedure go into effect? I thought it used to be just the Attorney General.

Mr. MARONEY. It used to be the Director of the FBI to the Attorney General. It has been in the last six months or a year I believe, that new procedure has been adopted.

Senator KENNEDY. What criteria does the Assistant Attorney General use? What kind of instructions does he receive from the Attorney General in connection with his examination?

Mr. MARONEY. I do not know.

Senator KENNEDY. Whom does he consult with? Does he consult with you?

Mr. MARONEY. No, he consults with the Attorney General.

Senator KENNEDY. Under this new procedure, would the Assistant Attorney General consult with any career people in the Department

at all, or is it just he and the Attorney General? Does he consult with you, for example?

Mr. MARONEY. I do not know of any instance in which I have been consulted on one of these.

Senator KENNEDY. As I understand it, there is a rather dramatic difference in the handling of the crime detection taps, is there not?

Mr. MARONEY. Title III?

Senator KENNEDY. Yes. Mr. Henry Petersen, who is now the Assistant Attorney General for the Criminal Division, has described a rather elaborate procedure that is followed on title III taps, he spelled out in some detail the Department's review procedures for title III taps, and I thought they were extremely impressive.

Mr. Peterson told the Judiciary Committee in February:

> First of all, extensive instructions have been provided to all of the investigative agencies and to all of the attorneys as to the minute requirements of a very technical statute.
>
> Secondly, no request is entertained unless it is suggested by the investigative agency which in conjunction with the attorneys on the scene prepare very minute and extensive records in terms of probable cause, not only to believe that a crime has been committed, and not only that other techniques are not available to develop evidence with respect to the crime, but also to reflect that the particular instrumentality or device will be used and therefore the premise should be subject to electronic surveillance.
>
> That recommendation is first prepared by the attorneys in conjunction with the investigators and then reviewed by a staff attorney in a special section designed for that purpose, reviewed by the section chief, it is forwarded by the chief to the Deputy Assistant Attorney General, and the Deputy Assistant Attorney General sends a memorandum to the Attorney General recommending in favor if that be his view. We very seldom send any recommendation up against wiretapping; if we are of that view, we send them back for more work.
>
> It then goes to the Attorney General's Office and upon his approval, upon the approval of the Office, the document comes back and then is executed by the Assistant Attorney General, or one of his deputies, and that constitutes the authorization to the attorney to make application in the court for an order to authorize electronic eavesdropping, and, of course, needless to say, since a court order is required, the approval of the court of that application submitted is necessary before the device can become operative.
>
> Now, the statute provides that the order may provide for interception of conversations for a 30-day period and in no instance has the Department of Justice authorized interception in the initial order for longer than 15 days, but supposing that it becomes necessary, we can make a request for an extension through the court to extend it for an additional 15 days.

That is a rather elaborate procedure in which career and professional people are involved. The procedure that you have outlined—

Mr. MARONEY. Well, these situations would go through as elaborate a process in the FBI—the person originating it, the investigative agent, his supervisor. If he were in the field, the special agent in charge; the supervisor here at headquarters, the Assistant Director in charge of the particular division, and subsequently, by the Director of the FBI. So at that stage of the thing, you have substantial review and input by career professionals.

Senator KENNEDY. Are there any agencies other than the FBI which conduct national security wiretapping?

Mr. MARONEY. No, sir. Under the directive of President Johnson in 1965, all such wiretaps have to be approved personally by the Attorney General and are conducted by the FBI.

Senator KENNEDY. Well, why would Mr. Hoover have said in his House Appropriations Committee appearance this past March, "In the security field, we are operating 34 telephone surveillances and 6 microphone surveillances in FBI cases." That seems to imply that other agencies and bureaus are also doing some tapping.

Mr. MARONEY. Well, all electronic surveillance in the national security area is handled by the FBI after first being approved by the Attorney General.

Senator KENNEDY. Does the Justice Department ever use private agencies to do any tapping for them?

Mr. MARONEY. No, sir; not to my knowledge.

Senator KENNEDY. Have you ever used information that has been gathered by private agencies?

Mr. MARONEY. I do not know whether it has ever happened. I do not know whether somebody may have somewhere along the years come in with——

Senator KENNEDY. Is there a rule against it?

Mr. MARONEY. Well, I can't cite you any particular rule, but the FBI is the investigative agency for the Department of Justice and I know of no situation where any private outfit has been asked to aid in that regard.

Senator KENNEDY. I have just a very few more, then we will hear from Ramsey Clark if that is all right.

We have to vote again. We will recess for 10 minutes.

[Recess.]

Senator KENNEDY. The subcommittee will come to order.

Given the *Keith* decision, what review will now be made of pending cases? Will there be a review now of some of the pending cases that might be affected by the *Keith* decision?

Mr. MARONEY. Yes, sir. In each of those cases, a determination will have to be made whether to turn over the logs in instances which are affected by the *Keith* decision.

Senator KENNEDY. How about individuals who have been prosecuted and convicted and perhaps even jailed as a result of information that we now find was unconstitutionally obtained. Are you making any effort to try to make those defendants aware of that?

Mr. MARONEY. Well, for years now, going back to the *Alderman* case, we had been making disclosures to the court in camera in every one of these instances. So the fact of overhearing in any case has been brought to the attention of the defendant and the court. There is no danger of any conviction having gone by in which motions were made as they are in practically all cases without the government having made a disclosure—at least to the court in camera.

Senator KENNEDY. What about the fellow who is sitting in jail today? Do you make any effort to notify him?

Mr. MARONEY. There should not be any sitting in jail who are unaware of any overhearing that was presented at the trial. It has been presented as a matter of course since the *Alderman* decision in about 1967.

Senator KENNEDY. Would that not only be true if he filed a motion?

Mr. MARONEY. That is right. But we would not even know it normally, unless he filed a motion which triggered a check.

Senator KENNEDY. Do you think you have any obligation to try to find out if there are people who are in jail, who have been convicted, but who had not filed a motion? Do you think you have any obligation to try to make them aware of their rights?

Mr. MARONEY. Well, he was, of course, represented at the time by counsel. His counsel apprised him of his rights and they took the remedies that were available to him, and presumably, if they were concerned about this area, they would have filed a motion and the government would have responded.

Senator KENNEDY. Of course, there might be circumstances where he did not know he was being tapped.

Mr. MARONEY. That is right. That is frequently the case. But an attorney representing a defendant makes the motion.

Senator KENNEDY. What about State cases, tainted State convictions? For example, where national security wiretap information has been given to local police or State prosecutors. Is there any chance that people could have been convicted by State court on this kind of information?

Mr. MARONEY. I do not know of any such instance.

Senator KENNEDY. Suppose there was some illegally obtained evidence and local authorities acted upon it, and then there was a conviction and a fellow was put into jail. Mabe the State officials do not even know that the information made available to them was illegally obtained. Maybe the Federal agents had said, "We have this information, but do not ask any questions about how we got it."

Mr. MARONEY. Well, I think you have the same situation. If he made motions at the time of the court proceedings, the court required a showing as to any information which the local authorities may have received from the FBI, the court has a remedy either to require disclosure or to dismiss the criminal case. And it has arisen a few times to my own information in connection with local trials. And the court asks for a response as to whether or not the defendant had been overheard by the Federal Government during a particular time frame. And we have on some occasions answered with respect to those requests by the court.

Senator KENNEDY. What is the Department's position on the defense of civil damage suits?

Mr. MARONEY. Well, we have a number of such suits that are pending. We are in the process of formulating our legal defense. I think essentially, it will be that the conduct complained of was carried out by the Attorney General in the good faith exercise of his responsibilities, and within the frame of his responsibilities, and therefore, should not make him liable.

Senator KENNEDY. Where do you find that good faith defense in the 1968 law?

Mr. MARONEY. Well, as I have indicated, we are presently formulating—we have not finished formulating our legal position in defense of those civil actions. We probably will have a brief prepared on that subject within the next 30 days. I would be glad to submit it for you.

Senator KENNEDY. Would you?

Mr. MARONEY. Yes, sir.

[Subsequent to the hearings, the following letter and materials were submitted by Mr. Maroney for the record:]

U.S. DEPARTMENT OF JUSTICE,
Washington, D.C., February 15, 1973.

Mr. MIKE EPSTEIN,
Senate Subcommittee on Administrative Practice and Procedure, U.S. Senate, Washington, D.C.

DEAR MIKE: This is in reply to your telephone request of yesterday concerning some additional materials I was to furnish the Committee as a result of my testimony on national security wiretapping sometime ago.

Enclosed are copies of a number of Answers to Complaints in pending cases as well as a Motion to Dismiss in the case of *Zweibon* v. *Mitchell, et al.* These documents set forth the basic position the government will be taking as a matter of defense in this type of suit. Most of these cases are in the discovery stage and we have not filed a Motion for Summary Judgment in any case, though we anticipate doing that in the near future in one or more of the cases. Of course, the Motion for Summary Judgment will be accompanied by a legal memorandum in support of the positions being taken.

I hope the enclosures satisfy the requirements of the Committee at the present time.

Sincerely,

KEVIN T. MARONEY,
Deputy Assistant Attorney General,
Internal Security Division.

Enclosures.

U.S. DISTRICT COURT FOR THE DISTRICT OF COLUMBIA
Civil Action No. 1879–72

DANIEL ELLSBERG, ET AL., PLAINTIFFS, *v.* JOHN N. MITCHELL, ET AL., DEFENDANTS.

AMENDED ANSWER TO COMPLAINT

Come now the defendants, by their undersigned attorneys, and pursuant to the provisions of Rule 15(a), Federal Rules of Civil Procedure, amend their Answer to Complaint, served and filed herein on January 26, 1973, as a matter of course, as follows:

FIRST DEFENSE

The national security surveillance of the telephone installation referred to in paragraphs 4 through 6 of the Complaint was authorized by the President of the United States, acting through the Attorney General, in the exercise of his authority relating to the Nation's foreign affairs and was deemed necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States and to protect national security information against foreign intelligence activities and as such was lawful and not violative of any provision of the Constitution of the United States or the provision of any Federal statute.

SECOND DEFENSE

The Court lacks jurisdiction over the subject matter of this action; plaintiffs lack standing to sue.

THIRD DEFENSE

Until January 20, 1969 Ramsey Clark was the Attorney General of the United States; from January 20, 1969 to March 1, 1972 defendant John N. Mitchell, was the Attorney General of the United States; on March 2, 1972 defendant Richard G. Kleindienst became the Acting Attorney General of the United States and, on June 12, 1972, the Attorney General of the United States. Until May 2, 1972 J. Edgar Hoover was the Director of the Federal

Bureau of Investigation; on May 3, 1972 defendant L. Patrick Gray, III became the Acting Director of the Federal Bureau of Investigation. Until August 12, 1968 John Finlator and Henry Giordano were Associate Directors of the Bureau of Narcotics and Dangerous Drugs; on August 12, 1968 defendant John E. Ingersoll became Director of the Bureau of Narcotics and Dangerous Drugs. Until August 5, 1969 Lester D. Johnson was Commissioner of the Bureau of Customs; from August 5, 1969 to May 2, 1972 Myles J. Ambrose was the Commissioner of the Bureau of Customs; on May 2, 1972 defendant Vernon D. Acree became the Commissioner of the Bureau of Customs. Until January 20, 1969 Sheldon Cohen was the Commissioner of the United States Internal Revenue Service; from January 21, 1969 until March 31, 1969 William H. Smith was the Acting Commissioner of the United States Internal Revenue Service; from April 1, 1969 to June 22, 1971 Randolph W. Thrower was the Commissioner of the United States Internal Revenue Service; from June 23, 1971 to August 5, 1971 Harold T. Swartz was the Acting Commissioner of the United States Internal Revenue Service: on August 6, 1971 Johnnie M. Walters became the Commissioner of the United States Internal Revenue Service. Until January 22, 1969 Dean Rusk was the secretary of State of the United States; on January 22, 1969 defendant William P. Rogers became the Secretary of State of the United States. Until January 20, 1969 Clark Clifford was Secretary of Defense of the United States; between January 20 and January 22, 1969 Stanley R. Resor was the Acting Secretary of Defense of the United States; on January 22, 1969 defendant Melvin R. Laird became the Secretary of Defense of the United States. At all times material herein defendant James J. Rowley has been he Director o the United States Secret Service and defendant Richard Helms has been the Director of the Central Intelligence Agency. All activities of the defendants in the premises were performed in furtherance of their official duties, were within the scope of their authority, and were not in excess of their statutory authority. Defendants are, therefore, absolutely immune from civil liability therefor under the doctrine of official immunity

FOURTH DEFENSE

The doctrine of sovereign immunity bars any suit against the United States where the United States has not consented to be sued. This suit is barred by the doctrine of sovereign immunity since it is in law and fact a suit against the United States to which the United States has not consented.

FIFTH DEFENSE

Until January 20, 1969 Ramsey Clark was the Attorney General of the United States; from January 20, 1969 to March 1, 1972 defendant John N. Mitchell, was the Attorney General of the United States; on March 2, 1972 defendant Richard G. Kleindienst became the Acting Attorney General of the United States and, on June 12, 1972, the Attorney General of the United States. Until May 2, 1972 J. Edgar Hoover was the Director of the Federal Bureau of Investigation; on May 3, 1972 defendant L. Patrick Gray, III became the Acting Director of the Federal Bureau of Investigation. Until August 12, 1968 John Finlator and Henry Giordano were Associate Directors of the Bureau of Narcotics and Dangerous Drugs; on August 12, 1968 defendant John E. Ingersoll became Director of the Bureau of Narcotics and Dangerous Drugs. Until August 5, 1969 Lester D. Johnson was Commissioner of the Bureau of Customs; from August 5, 1969 to May 2, 1972 Myles J. Ambrose was the Commissioner of the Bureau of Customs; on May 2, 1972 defendant Vernon D. Acree became the Commissioner of the Bureau of Customs. Until January 20, 1969 Sheldon Cohen was the Commissioner of the United States Internal Revenue Service; from January 21, 1969 until March 31, 1969 William H. Smith was the Acting Commissioner of the United States Internal Revenue Service; from April 1, 1969 to June 22, 1971 Randolph W. Thrower was the Commissioner of the United States Internal Revenue Service; from June 23, 1971 to August 5, 1971 Harold T. Swartz was the Acting Commissioner of the United States Internal Revenue Service; on August 6, 1971 Johnnie M. Walters became the Commissioner of the United States Internal Revenue Service. Until January 22, 1969 Dean Rusk was the Secretary of State of the United States; on January 22, 1969 defendant William P. Rogers became the Secretary of State of the United States. Until January 20, 1969 Clark Clifford was

Secretary of Defense of the United States; between January 20 and January 22, 1969 Stanley R. Resor was the Acting Secretary of Defense of the United States; on January 22, 1969 defendant Melvin R. Laird became the Secretary of Defense of the United States. At all times material herein defendant James J. Rowley has been the Director of the United States Secret Service and defendant Richard Helms has been the Director of the Central Intelligenge Agency. All activities of the defendants in the premises were performed in furtherance of their official duties, were undertaken in good faith and in the reasonable belief that such activities were necessary, lawful and within the scope of their authority. Defendants are, therefore, not liable to the plaintiffs in damages for such activity.

SIXTH DEFENSE

Plaintiffs' claims, contained in paragraphs 7 and 9 of the Complaint, that the overheard conversations referred to in paragraphs 4 through 6 of the Complaint included matters relevant to the defense of plaintiffs Ellsberg and Russo in *United States* v. *Anthony Joseph Russo, Jr. and Daniel Ellsberg, No.* 9373-CD-WMB (C.D. Calif., filed December 29, 1971) and that such surveillance also constituted a violation of the rights of plaintiffs Ellsberg and Russo to the effective assistance of counsel guaranteed by the Sixth Amendment have been previously and finally adjudicated and determined against plaintiffs Ellsberg and Russo and in favor of the Government in *Anthony J. Russo, Jr. and Daniel Ellsberg* v. *Honorable William Matthew Byrne, Jr., United States District Judge for the Central District of California,* No. 72-2306 (9th Cir., decided July 26, 1972), cert. denied, 41 L.W. 3271 (No. 72-307, November 13, 1972). The previous adjudication and determination of plaintiffs' claims aforesaid stand unreversed and unmodified and are in full force and effect. Said claims, therefore, were and are res judicata between plaintiffs and the defendants in this cause, and are barred by res judicata and the doctrine of collateral estoppel.

SEVENTH DEFENSE

Answering specifically the allegations contained in the numbered paragraphs of the Complaint, the defendants aver:

1. Defendants admit the allegations contained in paragraphs 1.a., 1.b., 1.c., 1.d., 1.e. and 1.f. of the Complaint.

2. Defendants admit the allegations contained in paragraphs 2.b., 2.c., 2.d., 2.e., 2.g., 2.h. and 2.i. of the Complaint. Defendants admit that defendant John N. Mitchell was Attorney General of the United States between January 20, 1969 and March 1, 1972, and that defendant Richard G. Kleindienst succeeded him as Attorney General of the United States. Defendants are not required to respond to the remaining conclusory allegations contained in paragraph 2.a. of the Complaint. Answering the allegation contained in paragraph 2.f. of the Complaint, defendants deny that "Charles Walters" is the Commissioner of the United States Internal Revenue Service and allege that Johnnie M. Walters is the Commissioner of the United States Internal Revenue Service. Defendants are not required to respond to the John Doe allegations contained in paragraph 2.j. of the Complaint.

3. Defendants deny the allegations contained in paragraph 3 of the Complaint.

4. Defendants deny that the "acknowledgement" pertained to "one or more" of plaintiffs' attorneys or consultants for the defense and allege that the July 21, 1972 *in camera* submission pertained to only one of plaintiffs' attorneys or consultants, as subsequently disclosed by the Court in *United States* v. *Russo* on July 25, 1972. Defendants admit the remaining allegations contained in paragraph 4 of the Complaint not inconsistent with defendants' denial and allegations herein.

5. Defendants admit the allegations contained in paragraph 5 of the Complaint, except that they allege that disclosure has been made to that Court *in camera.*

6. Defendants admit the allegations contained in paragraph 6 of the Complaint.

7. Defendants respectfully decline to respond to the allegations contained in paragraph 7 of the Complaint because either to admit or deny said allegations would reveal privileged information, except that defendants deny that any

overheard conversation of plaintiffs included matters relevant to the defense of plaintiffs Ellsberg and Russo.

8.–9. Defendants deny the allegations contained in paragraphs 8 and 9 of the Complaint.

WHEREFORE, defendants, having fully answered the allegations contained in the numbered paragraphs of the Complaint, respectfully pray that the Complaint herein be dismissed.

Respectfully submitted.

A. WILLIAM OLSON,
Assistant Attorney General.
EDWARD S. CHRISTENBURY,
Attorney, Department of Justice.
BENJAMIN C. FLANNAGAN,
Attorney, Department of Justice.

CERTIFICATE OF SERVICE

I certify that a copy of the foregoing Amended Answer to Complaint was served on the plaintiffs by mailing a copy thereof to their Attorney, David Rein, Esquire, FORER & REIN, 430 National Press Building, Washington, D.C. 20004 on January 29, 1973.

BENJAMIN C. FLANNAGAN,
Attorney, Department of Justice.
(Attorney for Defendants.)

U.S. DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

Civil Action No. 2083–72

KATHARINE C. WORDEN, PLAINTIFF, *v.* ROBERT DOLE, Chairman, Republican National Committee, GEORGE P. SHULTZ, Secretary of the Treasury, JAMES J. ROWLEY, Director, U.S. Secret Service, Treasury Department, RICHARD KLEINDIENST, Attorney General, Department of Justice, L. PATRICK GRAY III, Acting Director, Federal Bureau of Investigation, HOTEL FONTAINEBLEAU CORP., Miami Beach, Fla.; and JOHN DOE, DEFENDANTS.

ANSWER TO AMENDED COMPLAINT BY DEFENDANTS SHULTZ, ROWLEY, KLEINDIENST AND GRAY

Come now George P. Shultz, the Secretary of the Treasury of the United States, James J. Rowley, the Director of the United States Secret Service, Richard G. Kleindienst, the Attorney General of the United States, and L. Patrick Gray, III, the Acting Director of the Federal Bureau of Investigation, hereinafter the Federal defendants, by their undersigned attorneys, and in answer to the Amended Complaint herein filed, insofar as said allegations refer to them, say:

FIRST DEFENSE

The Amended Complaint fails to state a claim upon which relief can be granted.

SECOND DEFENSE

At all times material herein defendant George P. Shultz was the Secretary of the Treasury of the United States, defendant James J. Rowley was the Director of the United States Secret Service, defendant Richard G. Kleindienst was the Attorney General of the United States and defendant L. Patrick Gray, III was the Acting Director of the Federal Bureau of Investigation. All activities of the Federal defendants in the premises were performed in furtherance of their official duties, were within the scope of their authority, and were not in excess of their statutory authority. The Federal defendants are, therefore, absolutely immune from civil liability therefor under the doctrine of official immunity.

THIRD DEFENSE

The doctrine of sovereign immunity bars any suit against the United States where the United States has not consented to be sued. This suit, insofar as the allegations of the Amended Complaint refer to the Federal defendants, is barred by the doctrine of sovereign immunity since it is in law and fact a suit against the United States to which the United States has not consented.

FOURTH DEFENSE

At all times material herein defendant George P. Shultz was the Secretary of the Treasury of the United States, defendant James J. Rowley was the Director of the United States Secret Service, defendant Richard G. Kleindienst was the Attorney General of the United States and defendant L. Patrick Gray, III was the Acting Director of the Federal Bureau of Investigation. All activities of the Federal defendants in the premises were performed in furtherance of their official duties, were undertaken in good faith and in the reasonable belief that such activities were necessary, lawful and within the scope of their authority. The Federal defendants are, therefore, not liable to the plaintiff in damages for such activity.

FIFTH DEFENSE

Answering specifically the allegations contained in the numbered paragraphs of the Amended Complaint, the Federal defendants aver:

1. The Federal defendants admit that the jurisdiction of the Court is invoked as alleged in paragraph 1 of the Amended Complaint for the relief described therein, but deny that the Court has jurisdiction over them under 18 U.S.C. §2520, 28 U.S.C. §§1331, 1332, 1337, 1343 or 1357, or 42 U.S.C. §1985(3) or by reason of the First, Fourth, Ninth or Fourteenth Amendments to the Constitution of the United States or otherwise; and deny that the matter in controversy, exclusive of interest and costs, exceeds the value of $10,000. The Federal defendants deny that any action has been taken by them in violation of plaintiff's constitutional or other legal rights, deny that they are liable in damages to the plaintiff under said amendments and statutes or under any other provision of law, and deny that plaintiff is entitled to judicial relief in any form or fashion. The Federal defendants lack knowledge or information sufficient to form a belief as to the truth of the remaining allegations contained in paragraph 1 of the Amended Complaint.

2. The Federal defendants do not contest the allegations contained in paragraph 2 of the Amended Complaint.

3.–5. The allegations contained in paragraphs 3 through 5 of the Amended Complaint refer to defendants other than the Federal defendants. Accordingly, the Federal defendants neither admit nor deny the allegations contained in paragraphs 3 through 5 of the Amended Complaint.

6.–9. The Federal defendants admit the allegations contained in paragraphs 6 through 9 of the Amended Complaint.

10. The allegations contained in paragraph 10 of the Amended Complaint refer to defendants other than the Federal defendants. Accordingly, the Federal defendants neither admit nor deny the allegations contained in paragraph 10 of the Amended Complaint.

11. The Federal defendants deny the allegations contained in paragraph 11 of the Amended Complaint insofar as said allegations refer to them. The Federal defendants lack knowledge or information sufficient to form a belief as to the truth of the remaining allegations contained in paragraph 11 of the Amended Complaint.

12.–14. The Federal defendants lack knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraphs 12 through 14 of the Amended Complaint.

15.–16. The Federal defendants deny the allegations contained in paragraphs 15 and 16 of the Amended Complaint insofar as said allegations refer to them. The Federal defendants lack knowledge or information sufficient to form a belief as to the truth of the remaining allegations contained in paragraphs 15 and 16 of the Amended Complaint.

17.–21. The Federal defendants lack knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraphs 17 through 21 of the Amended Complaint.

22.–24. The Federal defendants deny the allegations contained in paragraphs 22 through 24 of the Amended Complaint insofar as said allegations refer to them. The Federal defendants lack knowledge or information sufficient to form a belief as to the truth of the remaining allegations contained in paragraphs 22 through 24 of the Amended Complaint.

25. The Federal defendants repeat and reallege every answer to paragraphs 12 through 23 of the Amended Complaint.

26. The Federal defendants deny the allegations contained in paragraph 26 of the Amended Complaint.

27. The Federal defendants repeat and reallege every answer to paragraphs 12 through 23 of the Amended Complaint.

28. The allegations contained in paragraph 28 of the Amended Complaint refer to defendants other than the Federal defendants. Accordingly, the Federal defendants neither admit nor deny the allegations contained in paragraph 28 of the Amended Complaint.

WHEREFORE, the Federal defendants, having fully answered the allegations contained in the numbered paragraphs of the Amended Complaint, respectfully pray that the Amended Complaint herein be dismissed.

Respectfully submitted.

A. WILLIAM OLSON,
Assistant Attorney General.
EDWARD S. CHRISTENBURY,
Attorney, Department of Justice.
BENJAMIN C. FLANNAGAN,
Attorney, Department of Justice.
(Attorneys for Defendants Shultz, Rowley, Kleindienst and Gray.)

CERTIFICATE OF SERVICE

I certify that copies of the foregoing Answer to Amended Complaint by Defendants Shultz, Rowley, Kleindienst and Gray were served on the plaintiff and on defendants 1, 2, 3 and 8 by mailing copies thereof to:

1. MELVIN L. WULF, Esquire; SANFORD JAY ROSEN, Esquire; JOHN H. F. SHATTUCK, Esquire—American Civil Liberties Union Foundation, 22 East 40th Street, New York, N. Y.
   BRUCE ROGOW, Esquire, City National Bank Building, suite 733, 25 West Flagler Street, Miami, Fla.
   Ms. HOPE EASTMAN, 410 First Street, Washington, D.C.
   Attorneys for Plaintiff.
2. FRED C. SCRIBNER, Jr., Esquire; E. VICTOR WILLETTS, Jr., Esquire—Scriber, Hall, Thornburg & Thompson, suite 1209, 1200 18th Street NW., Washington, D.C.
   Attorneys for Defendants Robert Dole and Republican National Committee.
3. KENNETH WELLS PARKINSON, Esquire; THOMAS PENFILED JACKSON, Esquire; JAMES P. SCHALLER, Esquire—Jackson, Gray & Laskey, 1828 L. Street NW., suite 1111, Washington, D.C.
   PAUL L. O'BRIEN, Esquire; W. FRANK STICKLE, Jr., Esquire; RALPH N. ALBRIGHT, Esquire—Hanson, O'Brien, Birney, Stickle & Butler, 888 17th Street NW., Washington, D.C.
   Attorneys for Defendant Committee for the Re-Election of the President.
4. JAMES J. BIERBOWER, Esquire; ALVIN B. DAVIS, Esquire—Bierbower & Rockefeller, 1625 K Street NW., Washington, D.C.
   Attorneys for Defendant Hotel Fontainebleau Corporation.

on December 13, 1972.

BENJAMIN C. FLANNAGAN
Attorney, Department of Justice.
(Attorney for Defendants Shultz, Rowley, Kleindienst and Gray.)

U.S. DISTRICT COURT EASTERN DISTRICT OF MICHIGAN

Civil Action No. 39065

ABDEEN M. JABARA, PLAINTIFF, *v.* L. PATRICK GRAY III, as Acting Director of the Federal Bureau of Investigation; RICHARD G. KLEINDIENST, Attorney General of the United States, Department of Justice, and Neil J. Welch, Special Agent-in-Charge, Detroit Office, Federal Bureau of Investigation, Detroit, Michigan, and WINSTON CHURCHILL, JOHN DOE, RICHARD ROE, Special Agents, Detroit Office, Federal Bureau of Investigation, DEFENDANTS

ANSWER TO COMPLAINT

Come now the defendants, by their undersigned attorneys, and in answer to the Complaint herein filed, say:

FIRST DEFENSE

The Complaint is insufficient to create the case or controversy required under Article III of the Constitution to invoke the subject matter jurisdiction of the Court.

SECOND DEFENSE

The Complaint fails to state a claim upon which relief can be granted.

THIRD DEFENSE

The doctrine of sovereign immunity bars any suit against the United States where the United States has not consented to be sued. This suit is barred by the doctrine of sovereign immunity since it is in law and fact a suit against the United States to which the United States has not consented.

FOURTH DEFENSE

On March 2, 1972 defendant Richard G. Kleindienst became the Acting Attorney General of the United States and, on June 12, 1972, the Attorney General of the United States. Until May 2, 1972 J. Edgar Hoover was the director of the Federal Bureau of Investigation; on May 3, 1972 defendant L. Patrick Gray, III became the Acting Director of the Federal Bureau of Investigation. At all times material herein defendant Neil J. Welch has been the Special Agent in Charge of the Detroit office of the Federal Bureau of Investigation and defendant Winston T. Churchill has been a Special Agent of the Federal Bureau of Investigation. All activities of the defendants in the premises were performed in furtherance of their official duties, were within the scope of their authority, and were not in excess of their statutory authority. The defendants are, therefore, absolutely immune from civil liability therefor under the doctrine of official immunity.

FIFTH DEFENSE

On March 2, 1972 defendant Richard G. Kleindienst became the Acting Attorney General of the United States and, on June 12, 1972, the Attorney General of the United States. Until May 2, 1972 J. Edgar Hoover was the Director of the Federal Bureau of Investigation; on May 3, 1972 defendant L. Patrick Gray, III became the Acting Director of the Federal Bureau of Investigation. At all times material herein defendant Neil J. Welch has been the Special Agent in Charge of the Detroit office of the Federal Bureau of Investigation and defendant Winston T. Churchill has been a Special Agent of the Federal Bureau of Investigation. All activities of the defendants in the premises were performed in furtherance of their official duties, were undertaken in good faith and in the reasonable belief that such activities were necessary, lawful and within the scope of their authority. Defendants are, therefore, not liable to the plaintiffs in damages for such activity.

SIXTH DEFENSE

This suit, to the extent the Complaint seeks declaratory and injunctive relief to obtain the disclosure of the contents of the investigative files of the Federal

Bureau of Investigation and to regulate the investigative activities of the Federal Bureau of Investigation, is barred by the doctrines of separation of powers and executive privilege.

SEVENTH DEFENSE

Answering specifically the allegations contained in the numbered paragraphs of the Complaint, the defendants aver:

1. Defendants deny the allegations contained in paragraph 1 of the Complaint.

2. Defendants admit the allegations contained in paragraph 2 of the Complaint.

3. Defendants admit that the suit purports to be against them in their official capacities for their official activities, but deny all allegations contained in paragraph 3 of the Complaint and elsewhere which charge that said defendants have in any form or fashion acted in violation of plaintiff's constitutional or other legal rights, or that they have actetd with such a purpose, or that their actions have had such an effect.

4. Defendants deny the allegations contained in paragraph 4 of the Complaint.

5. Defendants admit that the Federal Bureau of Investigation has information concerning plaintiff obtained through normal investigative methods and practices, but deny that the Federal Bureau of Investigation has illegally obtained such information concerning plaintiff and further deny that the purpose of obtaining such information has been to gather "information about the plaintiff which relates exclusively to lawful and peaceful activities protected by the First Amendment." Defendants deny all allegations contained in paragraph 5 of the Complaint inconsistent therewith.

6. Defendants deny the allegations contained in paragraph 6 of the Complaint.

7. Defendants admit that information regarding speaking engagements of the plaintiff was obtained by the Federal Bureau of Investigation from individuals, including Special Agents, who were in attendance at meetings and gatherings where plaintiff was a speaker, but deny that the Federal Bureau of Investigation has illegally obtained such information concerning plaintiff and further deny that the purpose or effect of obtaining such information has been to violate plaintiff's constitutional rights. Defendants deny all allegations contained in paragraph 7 of the Complaint inconsistent therewith.

8. Defendants admit that the Federal Bureau of Investigation has made inquiry to ascertain the existence and locations of plaintiff's bank accounts and that such inquiries were made without plaintiff's knowledge and approval. Defendants deny that such inquiries were improper or unlawful or that legal process was required therefor. Defendants deny that the Federal Bureau of Investigation has illegally obtained any information relating to plaintiff's bank accounts in violation of his constitutional rights. Defendants deny all allegations contained in paragraph 8 of the Complaint inconsistent therewith.

9–14. Defendants deny the allegations contained in paragraphs 9 through 14 of the Complaint.

WHEREFORE, the defendants, having fully answered the allegations contained in the numbered paragraphs of the Complaint, respectfully pray that the Complaint herein be dismissed.

Respectfully submitted.

A. WILLIAM OLSON,
Assistant Attorney General.
RALPH G. GUY, JR.,
U.S. Attorney.
FRED M. MESTER,
Assistant U.S. Attorney.
EDWARD S. CHRISTENBURY,
Attorney, Department of Justice.
BENJAMIN C. FLANNAGAN,
Attorney, Department of Justice.
(Attorneys for Defendants.)

U.S. DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

Civil Action No. 2025–71

BERTRAM ZWEIBON et al., PLAINTIFFS, *v.* JOHN N. MITCHELL et al., DEFENDANTS.

ANSWER TO COMPLAINT

Come now the defendants, by their undersigned attorneys, and in answer to the complaint filed herein, state:

FIRST DEFENSE

The national security surveillance of a telephone installation at the office of the Jewish Defense League in the City of New York during the periods between October 1 through 31, 1970 and January 7 through June 30, 1971, was authorized by the President of the United States, acting through the Attorney General in the exercise of his authority relating to the nation's foreign affairs and was deemed essential to protect this nation and its citizens against hostile acts of a foreign power and to obtain foreign intelligence information deemed essential to the security of the United States and as such was lawful and not violative of any provision of the Constitution of the United States or the provision of any Federal statute.

SECOND DEFENSE

The Court lacks jurisdiction over the subject matter of this action.

THIRD DEFENSE

Plaintiffs lack standing to sue.

FOURTH DEFENSE

The Complaint fails to present a justiciable case or contorversy.

FIFTH DEFENSE

At all times material herein defendant John N. Mitchell was the Attorney General of the United States and defendants Barrett, Camire, Doherty, Drabik, Gausky, Holland, Patterson, Sodolak, and Sweeney were agents or employees of the Federal Bureau of Investigation acting under the direction of the Attorney General. All activities of the defendants in the premises were performed in furtherance of their official duties and were within the scope of their authority, were constitutional and not in excess of their statutory authority. Defendants are, therefore, absolutely immune from civil liability therefor under the doctrine of officical immunity.

SIXTH DEFENSE

The doctrine of sovereign immunity bars any suit against the United States where the United States has not consented to be sued. This suit is barred by the doctrine of sovereign immunity since it is in law and fact a suit against the United States to which the United States has not consented.

SEVENTH DEFENSE

The Complaint fails to state a claim upon which relief can be granted.

EIGHTH DEFENSE

The Complaint fails to state a claim upon which relief can be granted in a class action.

NINTH DEFENSE

Answering specifically the allegations contained in the numbered paragraphs of the complaint, the defendants aver:

1. Defendants admit that the action purports to be a damage action for unlawful interception of wire communication brought under the provisions of

18 U.S.C. §2520, 42 U.S.C. §1983 and 1985, and the Fourth Amendment of the Constitution, as alleged in the first and second sentences of paragraph 1 of the Complaint, but deny that any action has been taken by defendants in violation of plaintiffs' constitutional or other legal rights and further deny that defendants are liable in damages to the plaintiffs under said statutes and amendment or any other provision of law; and further deny that the Court has jurisdiction over this cause under the provisions of 28 U.S.C. §1331 and 1343, as alleged in the second sentence of paragraph 1 of the Complaint, or otherwise.

2. Answering the allegations contained in the first sentence of paragraph 2 of the Complaint, defendants admit that the action purports to be a class action, but deny that the plaintiffs and others sought to be represented by plaintiffs constitute a class within the meaning of Rule 23 of the Federal Rules of Civil Procedure and further deny that this action is maintainable under Rule 23(b)(1), (2), or (3). Answering the allegations contained in the second sentence of paragraph 2 of the Complaint, defendants admit that between October 1 and October 31, 1970, and January 7, 1971 and June 30, 1971, a national security surveillance of a telephone installation was conducted at the office of the Jewish Defense League in the City of New York and that such surveillance was authorized by the President of the United States, acting through the Attorney General in the exercise of his authority relating to the nation's foreign affairs and was deemed essential to protect this nation and its citizens against hostile acts of a foreign power and to obtain foreign intelligence information deemed essential to the security of the United States, during the course of which surveillance, as evidenced by the affidavit of the defendant John N. Mitchell, then Attorney General of the United States, dated June 7, 1971, filed in the United States District Court for the Eastern District of New York in the criminal cases of *United States* v. *Bieber, et al.* (71 Cr. 479) and *United States* v. *Joffe, et al.* (71 Cr. 480), which affidavit is annexed to the Complaint herein as Exhibit A, the conversations of plaintiffs Calderon, Cohen, Garfinkle and Meir D. Kahane were overheard. Defendants respectfully decline to answer further with respect to the remaining allegations contained in the second sentence of paragraph 2 of the Complaint because either to admit or deny the remaining allegations contained there would reveal privileged information.

3. Defendants lack knowledge or information sufficient to form a belief as to the truth of the allegations contained in the first clause of the first sentence of paragraph 3 of the Complaint. Defendants respectfully decline to answer the allegations contained in the second clause of the first sentence of paragraph 3 of the Complaint because either to admit or deny such allegations would reveal privileged information. Defendants deny the allegations contained in the second and third sentences of paragraph 3 of the Complaint and reallege their answer to the allegations contained in the first sentence of paragraph 2 of the Complaint.

4. Defendants reallege their answer to the allegations contained in the second sentence of paragraph 2 of the Complaint and respectfully decline to answer further the allegation contained in paragraph 4 of the Complaint because either to admit or deny such allegations beyond their answer to the allegations contained in the second sentence of paragraph 2 of the Complaint would reveal privileged information.

5. Defendants lack knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 5 of the Complaint.

6. Defendants admit the allegation contained in the first sentence of paragraph 6 of the Complaint, except that defendants deny that defendant John N. Mitchell is now the Attorney General. Defendants admit the allegations contained in the second sentence of paragraph 6 of the Complaint.

7. Defendants reallege their answer to the allegations contained in the second sentence of paragraph 2 of the Complaint and respectfully decline to answer further the allegations contained in paragraph 7 of the Complaint because either to admit or deny such allegations beyond their answer to the allegations contained in the second sentence of paragraph 2 of the Complaint would reveal privileged information.

8. Defendants reallege their answer to the allegations contained in the second sentence of paragraph 2 of the Complaint and respectfully decline to answer further the allegations contained in paragraph 8 of the Complaint because either to admit or deny such allegations beyond their answer to the

allegations contained in the second sentence of paragraph 2 of the Complaint would reveal privileged information.

9. Defendants reallege their answers to the allegations contained in the second sentence of paragraph 2 of the Complaint and in the second sentence of paragraph 6 of the Complaint and respectfully decline to answer further the allegations contained in paragraph 9 of the Complaint because either to admit or deny such allegations beyond their answers to the allegations contained in the second sentence of paragraph 2 of the Complaint and in the second sentence of paragraph 6 of the Complaint would reveal privileged information.

10. Defendants admit that Exhibit A to the Complaint is a true copy of the affidavit of defendant John N. Mitchell, then Attorney General of the United States, dated June 7, 1971, filed in the United States District Court for the Eastern District of New York in the criminal cases of *United States* v. *Bieber, et al.* (71 Cr. 479) and *United States* v. *Joffe, et al.* (71 Cr. 480). Defendants reallege their answers to the allegations contained in the second sentence of paragraph 2 of the Complaint and in the second sentence of paragraph 6 of the Complaint and respectfully decline to answer further the allegations contained in paragraph 10 of the Complaint because either to admit or deny such allegations beyond their answers to the allegations contained in the second sentence of paragraph 2 of the Complaint and in the second sentence of paragraph 6 of the Complaint would reveal privileged information.

11. Defendants reallege their answer to the allegations contained in the second sentence of paragraph 2 of the Complaint and respectfully decline to answer further the allegations contained in paragraph 11 of the Complaint because either to admit or deny such allegations beyond their answer to the allegations contained in the second sentence of paragraph 2 of the Complaint would reveal privileged information, except that they admit that said national security surveillance was not conducted pursuant to a court order.

12. Defendants reallege their answer to the allegations contained in the second sentence of paragraph 2 of the Complaint and respectfully decline to answer further the allegations contained in paragraph 12 of the Complaint because either to admit or deny such allegations beyond their answer to the allegations contained in the second sentence of paragraph 2 of the Complaint would reveal privileged information, except that they deny all allegations of unlawfulness or illegality contained in paragraph 12 of the Complaint.

13. Defendants reallege their answer to the allegations contained in the second sentence of paragraph 2 of the Complaint and respectfully decline to answer further the allegations contained in paragraph 13 of the Complaint because either to admit or deny such allegations beyond their answer to the allegations contained in the second sentence of paragraph 2 of the Complaint would reveal privileged information.

14. Defendants reallege their answer to the allegations contained in the second sentence of paragraph 2 of the Complaint and respectfully decline to answer further the allegations contained in paragraph 14 of the Complaint because either to admit or deny such allegations beyond their answer to the allegations contained in the second sentence of paragraph 2 of the Complaint would reveal privileged information, except defendants deny all allegations of unlawfulness or illegality and allege that plaintiffs are not entitled to judicial relief in any form or manner.

15. Defendants deny the allegations contained in paragraph 15 of the Complaint.

WHEREFORE, the defendants, having fully answered the allegations contained in numbered paragraphs of the Complaint, respectfully pray that the Complaint herein be dismissed.

Respectfully submitted.

A. WILLIAM OLSON,
Assistant Attorney General.
ROBERT L. KEUCH,
Attorney, Department of Justice.
BENJAMIN C. FLANNAGAN,
Attorney, Department of Justice.
PETER T. STRAUB,
Attorney, Department of Justice.
(Attorneys for Defendants.)

CERTIFICATE OF SERVICE

I certify that a copy of the foregoing Answer to Complaint was served on the plaintiffs by mailing copies thereof to their counsel, Herbert J. Miller, Esquire, and Nathan Lewin, Esquire, MILLER, CASSIDY, LARROCA AND LEWIN, 1320–19th Street, N.W., Suite 500, Washington, D.C. 20036 on July 28, 1972.

BENJAMIN C. FLANNAGAN,
Attorney, Department of Justice.
(Attorney for Defendants.)

U.S. DISTRICT COURT FOR THE DISTRICT OF COLUMBIA
Civil Action No. 2025–71

BERTRAM ZWEIBON et al., PLAINTIFFS, *v.* JOHN N. MITCHELL et al., DEFENDANTS.

MOTION TO DISMISS

Come now the defendants, by their undersigned attorneys, and respectfully move this Honorable Court, pursuant to the provisions of Rule 12(b)(6) of the Federal Rules of Civil Procedure, to dismiss this action on the ground that the Complaint fails to state a claim upon which relief can be granted.

In support of this motion the Court's attention is respectfully invited to the Complaint and the exhibit attached thereto and to defendants' attached Memorandum of Points and Authorities in Support of Defendants' Motion to Dismiss.

Respectfully submitted.

ROBERT C. MARDIAN,
Assistant Attorney General.
BENJAMIN C. FLANNAGAN,
Attorney, Department of Justice.
PETER T. STRAUB,
Attorney, Department of Justice.
(Attorneys for Defendants.)

CERTIFICATE OF SERVICE

I certify that a copy of the foregoing Motion to Dismiss was served on the plaintiffs by mailing a copy thereof to their attorney, Nathan Lewin, Esquire, Miller, Cassidy, Larroca & Lewin, 1320 19th Street, N.W., Suite 500, Washington, D.C. 20036 on this 7th day of December, 1971.

BENJAMIN C. FLANNAGAN,
Attorney, Department of Justice.
(Attorney for Defendants.)

U.S. DISTRICT COURT FOR THE DISTRICT OF COLUMBIA
Civil Action No. 2025–71

BERTRAM ZWEIBON et al., PLAINTIFFS, *v.* JOHN N. MITCHELL, et al., DEFENDANTS.

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS

STATEMENT

This is a civil action for money damages. The defendants are the Attorney General of the United States and nine Special Agents and Employees of the Federal Bureau of Investigation of the United States Department of Justice. Jurisdiction is alleged to be under 28 U.S.C. 1331 (a) and 1343. The claim is alleged to arise under 18 U.S.C. 2520, 42 U.S.C. 1983 and 1985 and the Fourth Amendment of the Constitution of the United States. There is no formal allegation that the amount in controversy exceeds, exclusive of interest and costs, the sum of $10,000.

Plaintiffs' claim for money damages is predicated entirely and exclusively on alleged telephonic surveillance of them occurring during the course of a national security surveillance of a telephone installation at the offices of the Jewish Defense League in New York City during the periods between October 1 through 31, 1970, and January 7 through June 30, 1971, which "was authorized by the President of the United States, acting through the Attorney General in the exercise of his authority relating to the nation's foreign affairs and was deemed essential to protect this nation and its citizens against hostile acts of a foreign power and to obtain foreign intelligence information deemed essential to the secucrity of the United States." Complaint, Exhibit A (Affidavit of the Attorney General).

ARGUMENT

1. *The Complaint does not state a claim for relief under any Act of Congres providing for the protection of civil rights.*

There is no substantial allegation that plaintiffs are entitled to relief under any Act of Congress providing for the protection of civil rights. Plaintiffs have not alleged under 42 U.S.C. 1985 " * * * facts amounting to intentional and purposeful discrimination to the plaintiffs individually or as members of a class," *Norton* v. *McShane*, 332 F. 2d 855, 863 (5th Cir. 1964), cert. denied, 380 U.S. 981(1965); *Lombardi* v. *Peace*, 259 F. Supp. 222, 225 (S.D.N.Y. 1966), and their claim under 28 U.S.C. 1343 must therefore be dismissed. See *Giancana* v. *Johnson*, 335 F. 2d 366, 369, n.9 (7th Cir. 1964), cert. denied, 379 U.S. 1001 (1965).

As the Supreme Court pointed out in *Snowden* v. *Hughes*, 321 U.S. 1, 10 (1944), the "lack of any allegation in the complaint * * * tending to show a purposeful discrimination between persons or classes of persons is not supplied by the [use of] opprobrious epithets * * * or by characterizing [the complained of action] as unequal, unjust and oppressive * * *". See also, *McGuire* v. *Todd*, 198 F. 2d 60 (5th Cir. 1952); *Morgan* v. *Sylvester*, 125 F. Supp. 380 (S.D.N.Y. 1954); and *Jennings* v. *Nester*, 217 F. 2d 153 (7th Cir. 1954). In short, it is not enough to allege that the defendants acted unconstitutionally; rather, plaintiffs must show that "every citizen * * * [was] * * * not potentially subject to the same treatment." *Jennings* v. *Nester*, *supra*, 217 F. 2d at 154. This, plaintiffs have failed to do, and the Complaint fails to state a claim under 42 U.S.C. 1985.

Nor, does the Complaint state a claim under 42 U.S.C. 1983, for there is no suggestion that any action taken by the defendants was "under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory". See *Norton* v. *McShane*, *supra*, 332 F. 2d at 862.

2. *The Complaint does not state a claim for relief under 18 U.S.C. 2520 or the Fourth Amendment.*

There is no formal allegation in the complaint that the amount in controversy exceeds, exclusive of interest and costs, the sum of $10,000. See 28 U.S.C. 1331(a). However, in view of the prayer for money damages in excess of that amount, we will treat this as an oversight, inasmuch as the presence or absence of such an allegation is of no moment in this litigation.

Apart from their civil rights claim, plaintiffs look to the provisions of 18 U.S.C. 2520 and the Fourth Amendment of the Constitution as bases for the recovery of money damages. But neither affords them grounds for relief.

a. *18 U.S.C. 2520*

Section 2520 of the Omnibus Crime Control and Safe Streets Act of June 10, 1968, 18 U.S.C. 2520, provides:

> Any person whose wire or oral communication is intercepted, disclosed or used *in violation of this chapter* shall (1) have a civil cause of action against any person who intercepts, discloses or uses, or procures any other person to intercept, disclose, or use such communications and (2) be entitled to recover from any such person—
>
> (a) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1000, whichever is higher;
>
> (b) punitive damages; and
>
> (c) a reasonable attorney's fee and other litigation costs reasonably incurred.

> A good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under this chapter or any other law. (Emphasis supplied.)

Section 2511(3) of the same chapter, 18 U.S.C. 2511(3), provides, in part:

> Nothing contained in this chapter or in Section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against * * * or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or * * *.

Thus the threshold question here is whether the activity described in Section 2511(3) is activity which violates chapter 119 of the Act (18 U.S.C. 2510–2520), for if it does not, no civil cause of action was created under Section 2520 for such conduct, inasmuch as "the scope of the remedy" under Section 2520 "is intended to be both comprehensive and exclusive". Senate Report No. 1097, 2 U.S. Code, Cong. & Adm. News, 1968, 2112, at 2196.

This threshold question has been answered in the negative by Judge Ferguson in *United States* v. *Smith*, 321 F. Supp. 424 (C.D. Calif. 1971), where he stated at 425:

> The major thrust of the relevant portion of this Act makes electronic eavesdropping a federal crime punishable by a fine of $10,000, or imprisonment of up to five years, or both. However there are certain exceptions and under these limited circumstances electronic eavesdropping is not a federal crime. The portion quoted above [Section 2511(3)] provides for one of these exceptions. Thus the President does not commit a crime under this statute when he authorizes electronic surveillance "deemed essential to the security of the United States." * * *

Accordingly, inasmuch as the national security surveillance of a telephone installation at the offices of the Jewish Defense League "was authorized by the President of the United States, acting through the Attorney General in the exercise of his authority relating to the nation's foreign affairs and was deemed essential to protect this nation and its citizens against hostile acts of a foreign power and to obtain foreign intelligence information deemed essential to the security of the United States," Complaint, Exhibit A (Affidavit of the Attorney General), such telephone surveillance was *not* in violation of the Statute and therefore the Complaint fails to state a claim upon which relief can be granted under the provisions of 18 U.S.C. 2520.

b. *the Fourth Amendment*

We believe that the Court has no occasion to consider here whether plaintiffs are entitled to recover money damages for an alleged violation of their rights under the Fourth Amendment of the United States Constitution, for we believe that the Congress, in enacting Section 2520 of the Omnibus Crime Control and Safe Streets Act of June 10, 1968, 18 U.S.C. 2520, created an exclusive remedy for the recovery of such damages, see the dissenting opinion of Chief Justice Burger in *Bivens* v. *Six Unknown Named Agents of the Federal Bureau of Narcotics*, 403 U.S. 388, 411, 422 (1971) (dissenting opinion), and Senate Report No. 1097, 2 U.S. Code, Cong. and Adm. News, 1968, *supra*, 2112, at 2196, and as we demonstrated above in part 2.a. of this argument, plaintiffs are not entitled to money damages under the provisions of that Statute.

However, if the Court concludes that plaintiffs' Fourth Amendment claims must be adjudicated, we respectfully submit that there has been no violation of plaintiffs' rights under the Fourth Amendment and that the Complaint fails to state a claim upon which relief can be granted on that theory of recovery.

The Courts have repeatedly ruled that a national security surveillance of a telephone installation which was authorized by the President of the United States, acting through the Attorney General in the exercise of his authority relating to the nation's foreign affairs and was deemed essential to protect the nation and its citizens against hostile acts of a foreign power and to obtain foreign intelligence information deemed essential to the security of the United States," Complaint, Exhibit A (Affidavit of Attorney General), is lawful and not violative of the Fourth Amendment or any other provision of the Constitution. See *United States* v. *Clay*, 430 F. 2d 165, 170–172 (5th Cir. 1970), reversed on other grounds, 403 U.S. 698 (1971); *United States* v. *Stone, Rosenbaum, et al.* 305 F. Supp. 75, 81–82 (D.D.C. 1969); *United States* v. *Butenko*

and Ivanov, —— F. Supp. —— (D.N.J., Criminal No. 418–68, opinion of Judge Augelli filed November 13, 1970) ; and *United States* v. *Hoffman*, —— F. Supp. —— (D.D.C., Criminal No. 973–71, opinion of Judge Smith filed November 23, 1971).

Accordingly, inasmuch as the national security surveillance of a telephone installation at the offices of the Jewish Defense League "was authorized by the President of the United States, acting through the Attorney General in the exercise of his authority relating to the nation's foreign affairs and was deemed essential to protect this nation and its citizens against hostile acts of a foreign power and to obtain foreign intelligence information deemed essential to the security of the United States, Complaint, Exhibit A (Affidavit of Attorney General), the Complaint fails to state a claim upon which relief can be granted under the provisions of the Fourth Amendment of the Constitution of the United States.

CONCLUSION

For the reasons stated, the defendants respectfulcly submit that the Court should grant defendants' Motion to Dismiss and dismiss the Complaint with prejudice.

Respectfully submitted.

ROBERT C. MARDIAN,
Assistant Attorney General.
BENJAMIN C. FLANNAGAN,
Attorney, Department of Justice.
PETER T. STRAUB,
Attorney, Department of Justice.
(Attorneys for Defendants.)

CERTIFICATE OF SERVICE

I certify that a copy of the foregoing Memorandum of Points and Authorities in Support of Defendants' Motion to Dismiss was served on the plaintiffs by mailing a copy thereof to their attorney, Nathan Lewin, Esquire, Miller, Cassidy, Larroca & Lewin, 1320 19th Street, N.W., Suite 500, Washington, D.C. 20036 on this 7th day of December, 1971.

BENJAMIN C. FLANNAGAN,
Attorney, Department of Justice.
(Attorney for Defendants.)

U.S. DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

Civil Action No. 2025–71

BERTRAM ZWEIBON et al., PLAINTIFFS, *v.* JOHN N. MITCHELL et al., DEFENDANTS.

DEFENDANTS' REQUEST FOR LEAVE OF COURT TO FILE SUPPLEMENTAL MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS

Come now the defendants, by their undersigned attorneys, and request leave of court to file the attached Supplemental Memorandum for the reason that Plaintiffs' Memorandum of Points and Authorities in Response to Defendants' Opposition to Plaintiffs' Motion for Class Action Order was not brought to the attention of the trial attorneys for defendants until after the filing of Defendants' Motion to Dismiss and the memorandum in support thereof, and plaintiffs have raised issues for which response is deemed necessary in their Memorandum.

The attention of this Honorable Court is respectfully directed to the attached Supplemental Memorandum of Defendants.

ROBERT C. MARDIAN,
Assistant Attorney General.
BENJAMIN C. FLANNAGAN,
Attorney, Department of Justice.
PETER T. STRAUB,
Attorney, Department of Justice.
(Attorneys for Defendants).

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Defendants' request for Leave or Court to File Supplemental Memorandum of Points and Authorities in Support of Defendants' Motion to Dismiss was served on counsel for the plaintiffs herein by mailing postage prepaid copies to Herbert J. Miller, Jr., Esquire and Nathan Lewin, Esquire, at the following address; Miller, Cassidy, Larroca and Lewin, 1320 19th Street N.W., Suite 500, Washington, D.C. 20036; on this 28th day of December, 1971.

PETER T. STRAUB,
Attorney, Department of Justice.
(Attorney for Defendants.)

U.S. DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

Civil Action No. 2025–71

BERTRAM ZWEIBON et al., PLAINTIFFS, *v.* JOHN N. MITCHELL et al., DEFENDANTS.

DEFENDANTS' SUPPLEMENTAL MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS

Plaintiffs seek disclosure of the materials in the possession of the government pertaining to the electronic surveillance for quite a number of reasons,[1] but the argument for the production of the documents is climaxed by this statement: "Clearly plaintiffs are entitled to production of the very materials in defendants' control establishing their damage claims as specified in 18 U.S.C. Section 2520", p. 10, Plaintiffs' Memorandum of Points and Authorities in Response to Defendants' Opposition of Plaintiffs' Motion for Class Action Order.

It is obvious that, at this stage of the proceedings in this case, determination of damages is premature, to say the least, since liability has not been established. Furthermore, the government believes nondisclosure is required because of the legality of the surveillance, the sensitivity of the documents, the disclosure of which would prejudice the national security, and the fact that the contents of the documents are totally immaterial and irrelevant to this law suit. Because the prior points have heretofore been fully developed, we will limit our argument to this last aspect of disclosure.

Each of the cases to which the defendants made reference and on which defendants relied to establish the point that foreign intelligence information electronic surveillance was legal are criminal cases[2] and in each the court conducted an *in camera* inspection of the documents and material produced

---

[1] At least the following reasons can be gleaned from Plaintiffs' Memorandum of Points and Authorities in Response to Defendants' Opposition to Plaintiffs' Motion for Class Action Order:

(1) Disclosure is necessary in order to decide whether plaintiffs have "a substantial possibility" of prevailing on the merits of the lawsuit (page 2);

(2) The criminal cases cited by defendants all included *in camera* inspection (pages 3–4);

(3) The government, in its brief before the Supreme Court in *Keith, infra,* has admitted that the actions of the Attorny General are not immune from judicial review (footnote, page 4);

(4) Limited review is necessary to test the "good faith" of the Attorney General (page 6);

(5) Disclosure is necessary to test the sworn statement of the Attorney General that the surveillance was pursuit to the gathering of foreign intelligence information (page 7);

(6) Disclosure is necessary to test the sworn statement of the Attorney General that to disclose the material would prejudice the national security (page 9);

(7) "Our adversarial [sic] system" requires more than an *in camera* inspection and dictates full disclosure to the plaintiffs (page 9) and

(8) Limited disclosure of a portion of the documents that has already been made in the criminal cases to which some of the plaintiffs were parties, and, albeit under a protective order of Judge Weinstein, there is therefor no further need for secrecy (pages 9–10).

[2] *United States* v. *Clay,* 430 F. 2d 165 (5th Circuit 1970), reversed on other grounds, 403 U.S. 698 (1971), *United States* v. *Stone,* 305 F. Supp. 75 (D.D.C. 1969), *United States* v. *Butenko,* 318 F. Supp. 66 (D.N.J. 1970), and *United States* v. *Hoffman,* 973–71, D.D.C., Order of Judge Smith dated November 23, 1971.

through the surveillance. Indeed, that was also the case in the criminal matters from which this case springs.[3] However, the issue for resolution by the *in camera* inspections and hearings held subsequently was whether the indictments grew out of the overhearings, and not whether the overhearings resulted from foreign intelligence gathering electronic surveillance. In other words, the courts conducted *in camera* inspections, and Judge Weinstein held a hearing in the *Joffe* and *Beiber* cases, for one purpose: To determine the relevancy of the surveillance to the criminal indictment.

Relevancy is not at issue in this civil lawsuit. The contents of the logs and airtels and other documents shed no light on the authorization of the Attorney General for the interceptions.

It has long been the rule in criminal cases that a search, with or without a warrant, is not to be tested by the results of that search. An improper search in which evidence is discovered is not thereby made proper; nor does the failure to discover evidence invalidate a proper search. Thus, the seizure is not to be considered as determinative of questions arising from the search.

Plaintiffs stress that disclosure was made in the criminal cases to which some of them were parties, *Joffe* and *Beiber*. They omit the protective order entered by Judge Weinstein on June 29, 1971:

"This Court having ordered the United States of America to furnish the defendants and their counsel, a copy of the written summaries of the conversations which were monitored pursuant to an electronic surveillance and the United States of America being prepared to produce said summaries to the defendants and their counsel; now therefore it is hereby

"Ordered, That the defendants and their counsel may not divulge the contents of any of the above-mentioned written summaries to any person without securing the prior approval of this court and that upon the completion of the legal proceedings in the case the said written summaries will be returned to the attorneys for the United States of America." [4]

Further, that hearing and disclosure came about in response to the criminal defendants' motion to suppress.

Thus, while the substantive language of the decisions cited has great bearing on the instant matter and establishes beyond question that the surveillance herein is legal and constitutional, the procedures followed by the trial courts in those criminal cases are inappropriate to this civil action, because of the significantly different questions and issues involved, and because of the particularized requirements of criminal cases.

The very nature of criminal cases gives rise to the limited judicial review of the actions of the Attorney General. Such review, while a normal outgrowth of a criminal case, nevertheless has no place in this civil suit:

"We make no contention that the Attorney General's action in concluding that a particular surveillance is necessary to protect the national security is immune from judicial review. Once the surveillance has been made, the courts may review it to determine its conformity with the standard of Fourth Amendment, just as they review any other search and seizure that is challenged in the criminal proceedings by a motion to suppress or an objection to evidence. * * *

"In determining the validity of the surveillance under the Fourth Amendment standard of reasonableness, the scope of judicial review should be extremely limited. Unless it appears that the Attorney General's determination that the proposed surveillance relates to a national security matter is arbitrary and capricious, i.e., that it constitutes a clear abuse of the broad discretion that the Attorney General has to obtain all information that will be helpful to the President in protecting the Government against 'overthrow' * * * by force or other unlawful means or against any other clear and present danger to [its] 'structure or existence' (Omnibus Crime Control and Safe Streets Act of 1968), the court should sustain it. The court should not substitute its judgment for that of the Attorney General on whether the particular organization, person or event involved has a sufficient nexus to protection of the national security to justify this surveillance."

---

[3] *United States* v. *Beiber et al*, 71–CR–479, and *United States* v. *Joffe et al*, 71–CR–480, D.E.N.Y., 1971.

[4] As a partial reason for the protective order, Judge Weinstein notes "that the government, I think properly, does not want to see these third parties embarrassed unnecessarily", page 10, transcript of proceedings, July 6, 1971 in *Joffe* and *Beiber*.

Pages 21, 22, Brief of the United States in *United States* v. *United States District Court for the Eastern District of Michigan, Southern Division and Honorable Damon J. Keith, October Term, 1971, No. 70–153.*

Based on the prior decisions in *Clay, Stone, Butenko,* and *Hoffman, supra,* it is the position of the defendants that the electronic surveillance in the instant case was legal and constitutional; there was no violation of the rights of plaintiffs; whatever the logs, airtels and other documents and materials pertaining to the surveillance may reveal, those documents, are irrelevant to these proceedings and nondisclosure is dictated for that reason, in addition to the affidavit of the Attorney General stating that disclosure would prejudice the national security of this country.

For the foregoing reasons, defendants move the court for an order dismissing plaintiffs' suit with prejudice.

ROBERT C. MARDIAN,
Assistant Attorney General.
BENJAMIN C. FLANNAGAN,
Attorney, Department of Justice.
PETER T. STRAUB,
Attorney, Department of Justice.
(Attorneys for Defendants.)

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Defendants' Supplemental Memorandum of Points and Authorities in Support of Defendants' Motion to Dismiss was served on counsel for the plaintiffs herein by mailing postage prepaid copies to Herbert J. Miller, Jr., Esquire and Nathan Lewin, Esquire, at the following address; Miller, Cassidy, Larroca and Lewin, 1320 19th Street NW., suite 500, Washington, D.C. 20036; on this 28th day of December, 1971.

PETER T. STRAUB,
Attorney, Department of Justice.
(Attorney for Defendants.)

U.S. DISTRICT COURT FOR THE DISTRICT OF COLUMBIA
Civil Action No. 2025–71

BERTRAM ZWEIBON et al., PLAINTIFFS, *v.* JOHN N. MITCHELL et al., DEFENDANTS.

SUPPLEMENT TO DEFENDANTS' ALTERNATIVE MOTION FOR STAY OF PROCEEDINGS

Defendants, by their undersigned attorneys, respectfully supplement defendants' alternative motion for stay of proceedings heretofore filed on November 22, 1971, and invite the attention of this Honorable Court to the attached Order of Judge Smith in *United States* v. *Hoffman,* D.D.C., Criminal No. 973–71, dated December 8, 1971.

ROBERT C. MARDIAN,
Assistant Attorney General.
BENJAMIN C. FLANNAGAN,
Attorney, Department of Justice.
PETER T. STRAUB,
Attorney, Department of Justice.
(Attorneys for Defendants.)

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Supplement to Defendants' Alternative Motion for Stay of Proceedings was served on counsel for the plaintiffs herein by mailing postage prepaid copies to Herbert J. Miller, Jr., Esquire and Nathan Lewin, Esquire, at the following address; Miller, Cassidy, Larroca and Lewin, 1320 19th Street NW., suite 500, on this 28th day of December, 1971.

PETER T. STRAUB,
Attorney, Department of Justice.
(Attorney for Defendants.)

93–045—73——4

Criminal No. 973–71

UNITED STATES, *v.* ABBOTT HOFFMAN, also known as ABBIE HOFFMAN

ORDER

Upon consideration of the motion for continuance filed on December 1, 1971 by the United States and the consent of defense counsel to that motion, it is this 8th day of December 1971

Ordered, That the motion of the United States for continuance be and it hereby is granted and all further proceedings in this case are hereby stayed pending the decision of the Supreme Court in the case of *United States v Keith*, No. 71–1105 (6th Cir., April 8, 1971), cert granted, 39 U.S.L.W. 3553 (June 22, 1971).

U.S. District Judge.

Senator KENNEDY. Getting back to one of my earlier questions—if you only have six devices which have been turned off because of the *Keith* decision, why is it such a burden to collect the tainted material and preserve it in such a way that you remove it from being available to those who have general access to the files? Why can't that material be gathered and assembled in one place—preserving it for the defense reasons you outlined, but removing it from the general files?

Mr. MARONEY. Well, the logs themselves could be isolated quite easily, and they are, as a matter of fact. But some of the information, of course, has gone into investigative files. It would be difficult to recall all of those. It would be a substantial administrative problem to do that.

Senator KENNEDY. Of course Justice Powell talked about that kind of problem in the *Keith* case—"Although some added burden will be imposed upon the Attorney General, this inconvenience is justified in a free society to protect constitutional values."

Could we get some determination on that? Could we request through you to the Attorney General that we get some response on that?

Mr. MARONEY. Yes, sir.

Senator KENNEDY. I want to thank you—unless Senator Hart has some questions——

Senator HART. No.

Senator KENNEDY. I want to thank you very much for coming, Mr. Maroney. Your responses have been extremely candid and forthright and you have been very helpful. There are a couple of points which are distressing to me. First of all there is the fact that the authorization decisions are being made in the Justice Department by two political appointees rather than by career and professional——

Mr. MARONEY. Well, that is the ultimate decision, Mr. Chairman. As I indicated, these are thoroughly reviewed at several levels in the FBI; there is a substantial career, professional input into these determinations.

Senator KENNEDY. But, of course, the FBI is the agency that is requesting the authority, not the one that is deciding whether to authorize the request. I think that that is an important distinction.

The second thing that concerns me is that this tainted information might be staying in the files. But as I understand it, you are going to provide us with some more information on that. Or you are going to make a request of the Attorney General to see what can be done about that.

But you have been personally very helpful. I want to commend you for your appearance here and the way that you have responded to these questions. It has been very valuable to us and to the Senate.

Mr. MARONEY. Thank you, Mr. Chairman.

Senator KENNEDY. Thank you very much.

[Subsequent to the hearing, the subcommittee received the following letter, dated Aug. 2, 1972, from Deputy Assistant Attorney General Maroney:]

U.S. DEPARTMENT OF JUSTICE,
Washington, D.C., August 2, 1972.

HON. EDWARD M. KENNEDY,
U.S. Senate,
Washington, D.C.

DEAR SENATOR KENNEDY: This is with reference to my testimony of June 29, 1972 before the Subcommittee on Administrative Practice and Procedure of the Senate Judiciary Committee on the subject of electronic surveillance. During the course of the testimony, you requested certain additional information which I have undertaken to secure as follows:

On page 29 of the reporter's transcript of the hearing on that date, you made a request for information on the length of operation of the six electronic surveillances in the national security field which were discontinued by the FBI as a result of the United States Supreme Court decision of June 19, 1972, in the *Keith* case. One of these electronic surveillances was operated for 21 months; two for 18 months; one for 4½ months; one for 3 months; and one for 2 weeks.

Of course, in accordance with established practice, those of the aforementioned surveillances which were in operation more than 3 months were reviewed and reauthorized every 3 months by the Attorney General.

On page 30 of the reporter's transcript, you requested a breakdown of the statutory categories under Title 18, U.S. Code, Section 2511.3, used by the Attorney General in authorization of the 27 electronic surveillances operated by the FBI as of June 29, 1972. Set forth below are the statutory categories and the number of times each category was used in the Attorney General's authorization of these 27 electronic surveillances. It should be noted that many of the authorizations were based on more than one statutory category.

Category:	*Electronic surveillances authorized under category*
Category 1—To protect the Nation against actual or potential attack or other hostile acts of a foreign power	2
Category 2—To obtain foreign intelligence information deemed essential to the security of the United States	23
Category 3—To protect national security information against foreign intelligence activity	15
Category 4—To protect the United States against the overthrow of the Government by force or other unlawful means	1
Category 5—Or against any other clear and present danger to the structure or existence of the Government	1

On pages 29 and 30 of the reporter's transcript there was a brief colloquy as to the method of computation of electronic surveillances, that is, when we say there are 27 electronic surveillances in effect on a given date does that represent "targets" or the number of devices. I am advised by the FBI that the number of surveillances indicated represent premises of organizations or individuals without regard to the number of instruments which may be involved in effectuating the surveillances.

The Committee further requested any written guidelines which had been issued by the Department as a result of the Supreme Court's decision in the *Keith* case. In view of the fact that almost all electronic surveillances now authorized by the Attorney General will be strictly in the area of foreign intelligence,

and since all requests for electronic surveillance authorizations are thoroughly screened within the Federal Bureau of Investigation and personally by the Attorney General, it is not believed necessary to promulgate any additional guidelines as a result of the *Keith* decision.

I hope the foregoing information will be of assistance to the Committee.

Sincerely,

KEVIN T. MARONEY,
Deputy Assistant Attorney General,
Internal Security Division.

Our next witness is Mr. Ramsey Clark. He is a former Attorney General of the United States. Mr. Clark, following his term as a distinguished Attorney General, has continued his interest in a wide range of different issues involving justice for the poor and powerless in our society, and has provided great assistance to this committee on a number of different issues. He has had a great deal of experience dealing with some of the matters which are before us here today.

We want to welcome you, Mr. Clark. We know that you had a very serious conflict in your schedule and that you adjusted it to be with us. We certainly appreciate those steps.

Senator Hart?

Senator HART. Mr. Chairman, may I, in addition to adding a word of welcome, offer a word of explanation to my witness? At 12:45 I am obliged to leave, but I am delighted that my 12:45 obligation follows your arrival. I can simply say amen to what the Chairman said.

Incidentally, while you have been sitting in the room this morning, it may not have come to your attention, a matter on which you and I have had some discussion over long years was decided by the Supreme Court. Did you get the word on the 5-to-4 decision on capital punishment?

STATEMENT OF RAMSEY CLARK, FORMER ATTORNEY GENERAL OF THE UNITED STATES

Mr. CLARK. Yes, I did.

Senator HART. Some days, there is good news.

Mr. CLARK. A glorious day for humanity by a margin of 5 to 4.

Thank you, Senator Kennedy, Senator Hart. It is always a great pleasure to appear before you.

Let me give some of the history of wiretapping and electronic surveillance as I know it. Unfortunately, our ignorance exceeds our knowledge in such subjects, because we practice government by secrecy, which in my opinion is wholly incompatible with a free society. The Bureau of Investigation was created in the Department of Justice in 1924. In February of 1931, at a time—when the regulation of the Bureau of Investigation provided that wiretapping would not be tolerated. Mr. Hoover disclosed that he knew of only three wiretaps as of that date conducted by the FBI during its history. Reminiscent of a sad dispute in the late 1960's, he explained he did not know about two of them until long after they were occurring when they occurred. As to the other one, he was instructed by the Attorney General of the United States to undertake the activity. As you might guess, the wiretaps were on the subjects of essentially

no importance. The first one occurred in 1926 in Indianapolis, Ind., in connection with an investigation under the Packers and Stockyards Act. The investigation itself was aborted. Two years later, Mr. Hoover found out the the wiretap had been initiated.

The second one had to do with an investigation of administrative irregularities at Leavenworth Penitentiary, where you should hardly need a wiretap to find out what prison officials were doing if you had any integrity in your institution.

The third one involved the Department of Justice itself. It seems that Attorney General Sargent had heard that it was possible to call certain phone numbers in the Department of Justice and order alcoholic beverages. This was during prohibition. A wiretap was put on those phones to see whether that was true.

During this period of time, 1924 to 1931, there was only one other investigative agency in the Department of Justice. That was the Bureau of Prohibition, which had to do with the enforced the prohibition laws. It apparently engaged rather freely in wiretapping, which gives you some sense of the priorities and importance that have been attached historically to this sort of business.

In the fall of 1931, Attorney General Mitchell—William D. Mitchell—caused the Bureau of Investigation over the opposition and the stated objection of Mr. Hoover, to authorize wiretapping for the first time in substantial and serious crimes where there was a great need.

The next significant reference to wiretapping arose from a dispute involving a prosecution in the city of Baltimore by the State of Maryland under its prostitution statutes. It developed that in an investigation of the Federal White Slave Act, the Mann Act, the FBI used a wiretap and turned information obtained from it over to the State for prosecution. A small scandal arose, as it should have.

In 1939 as World War II approached, legislation was proposed to authorize wiretapping. Mr. Hoover, who by then had directed the FBI for 15 years, reported that he thought wiretapping was "of very little value"—and that the risk of "abuse would far outweigh the value."

In March of 1940, Attorney General Robert H. Jackson, on the basis of an oral instruction followed later by a written instruction from President Franklin Roosevelt, advised the U.S. attorneys around the country that wherever wiretapping was employed, there was to be absolutely no use of any information gathered in any grand jury investigation or other prosecutorial effort. So you can say that from the very beginning of the use of wiretap in the foreign security field, it was recognized by the highest authority in the Department of Justice that there could be absolutely no use of the material gained in any prosecution. It is this fact that makes the opinion of Attorney General John Mitchell, first announced in the *Chicago Seven* case, so very dangerous and lawless. The notion that you could wiretap, that there was some inherent power in the executive by which it did not need a court order, and that finally, the very information so obtained could be used in prosecutions to seek convictions of people within this free society.

On May 21 1940, President Franklin Roosevelt issued his now famous order to Attorney General Robert H. Jackson. President Roosevelt said he agreed wholeheartedly with the Supreme Court decision in the *Nardone* case, but could not think, and he was, of course, right, that the court was then considering the risks the country faced from international conflict. Therefore, where there was substantial risk of international violence "grave matters involving the defense of the Nation" or subversion, he was ordering the use of wiretap. He said in the last paragraph of his letter that it should be limited to the "minimum" and limited "insofar as possible to aliens."

The scope of the use of electronic surveillance during the war is difficult to determine. Some indication of FBI use just before the war is given by the following. Between September 2 and October 2, 1941, in the months just before Pearl Harbor, the Federal Bureau of Investigation, asked Attorney General Francis Biddle to authorize seven wiretaps. Two were on persons who had some relation to Germany. One was an office, the German commercial attache, in New York City. Another was on a German citizen who had an automobile with a shortwave radio in it who drove around this country and down into Mexico.

Two had to do with Japanese. One was to be on the consulate at San Francisco. The other was to monitor all telephone calls from Hawaii to Japan. That request was made September 2, 1941.

The other three all involved alleged Communists. One was a young woman in San Francisco, one was a man who lived in North Hollywood, Calif., and the third—and this tells you what you need to know, I think—was a book store in Philadelphia. All but one of the wiretaps, bookstore in Attorney General Biddle's Philadelphia, were authorized. Most requests were pending for over a month before they were authorized.

In July 1946 Attorney General Tom Clark, consistent, he said in his memo to President Truman, with his two immediate predecessors, sought and obtained authority to tap—in areas that virtually affected domestic security this is the beginning of the cold war period.

President Eisenhower's first Attorney General, Herbert Brownell, affirmed and expanded that general authority in the 1950's. From that time, electronic surveillance grew like Topsy.

By June 30, 1945, there were extensive patterns of use. The requests in the national security area came primarily from the National Security Council, the National Security Agency, the Department of State, and from the FBI. On June 30, 1965, President Lyndon Johnson instructed that thereafter, all wiretaps within the United States should be approved by the Attorney General. We don't know wiretapping by our Government what goes on outside the United States.

My experience as Acting Attorney General and Attorney General with the national security area was that the requests involved chiefly the desire to know what foreign countries were doing. Distinctions between what we would consider friendly countries and unfriendly countries seemed to have little significance. Some wiretaps requested were not only outrageous, but potentially harmful. From time to

time a foreign delegation would come here to negotiate a treaty. Our officials might be interested to know what they were saying among themselves or communicating back to their nation. I refused to authorize that sort of tap. When foreign ministers came to this country wiretapping was sometimes sought. Over a period of several years, I turned down dozens of requests for taps on such foreign officials as agricultural attaches and tried to limit the authorizations I though the national security tap were wrong, but they had a long history and were, in my judgment, beyond my power to curtail at that time. To those areas where there was probable cause to believe that information might be obtained that would directly and significantly affect the capacity of a foreign nation to commit violence toward the United States.

I rationalized my policy in this way. It is inherent in political science that a Nation must have the power to protect itself from antisocial and criminal conduct within its borders. I believe this can, indeed must, always be done fairly. It is also inherent in political science that a nation's capacity to protect itself from sources of violence and aggression outside its borders is limited to military conflict. It can be very important to know about missile bases in Cuba or troop movements in parts of the world, and it can be important to know that techniques of destruction that have been developed in this country—which should not be developed but have been—are not falling into the hands of other people or nations. So that was the limitation that both my sense of history and of the usages of American law at that time permitted.

There was another area in which scores of requests for wiretap or bugs came before me. These related to domestic groups and individuals. Almost without exception, they involved the peace movement, student groups, or blacks. None were ever authorized while I was Attorney General. I did not believe it was either constitutionally permissible to use wiretap information in a prosecution when it was clear there was conduct that violated the laws of the United States and you had wiretapped a citizen, you would be powerless either to prosecute or to compel them to leave the country, and therefore, without sanction or remedy, to protect the public.

The range of people and groups was wide, unfocused, capricious. From time to time requests would be renewed by some of the groups and individuals.

I have seen in litigation, including litgation that I have been an attorney in, that there have been authorizations of wiretap or bugs on some of these individuals and some of these organizations since I left office.

My judgment is that anyone who has been overheard on an electronic surveillance has at the very least the right to know it and received the tapes or transcripts of the conversations. The destruction of the materials is hardly adequate to protect his rights. It seems to me, therefore, that there is at least a moral duty—it should be a legal duty—on the U.S. Department of Justice to inform everyone who has been overheard. It may be that there are people that government leaders fear and despise in this would-be nation of laws, who have been tapped. That would be all the more reason to let

them know that they were the subjects of such overhearing. We know that among those are some of the most benevolent among us, those who believe most deeply in this country and its true principles.

I do not think it is enough to rely on the *Dammon Keith* case. It is a milestone in the long road toward freedom, and perhaps a major one, but we have miles to go down that road even in this limited area of electronic surveillance and wiretap. Certainly there should be absolutely no use of wiretap or electronic surveillance without a court order under any circumstances.

Senator KENNEDY. You mean foreign as well as domestic?

Mr. CLARK. Foreign as well as domestic. Reluctantly, I have to say I cannot find any significant protection in a court warrant. In calendar 1971, out of more than 800 warrants applied for under title III of the Omnibus Crime Control Act of 1968, there was not a single rejection by a court. Now, that does not mean that the investigative agencies may not have wanted taps where approvals were not sought, so there may have been some inhibition at the precourt approval level. But my experience with life and the law tells me that it will always be possible for the executive to obtain warrants against individuals and groups in the domestic area who have created fear and hatred.

There should not be any extension in statutory authorization for warrants for such domestic groups. Of course, I think that the authorization of title III as it now exists should be repealed. I urged in 1968, essentially in the Right to Privacy Act, authorization that not be enacted in the first place.

We have heard this morning that only six taps have been taken off under the Department of Justices construction of the *Damon Keith* case. I do not know what that means. I assume that behind those six, if that is all there were, there must be 60 or perhaps considerably more that had been used but were discontinued before June 19. We have heard that there is at least one domestic organization that is still the subject of what has been called a national security tap without prior judicial approval. I would be very skeptical about the legality of that and have no skepticism about the desirability of it. I think it is undesirable and wrong.

Where we got the idea that there is some inherent integrity in certain members of the executive branch that will not be found in the judiciary or other branches, I do not know. There are single Federal agencies that have as many as 5,000 people with top secret clearance. They are really anonymous in this Nation and their number is legion and they can have access to the broadest range of what we call secret information, and if they have, I do not know why U.S. Senators should not; I do not know why U.S. district judges should not. Indeed, I do not know why U.S. citizens should not. I think the mischief and misery that we have caused with the notion that somehow or other, a free society can conduct important public business secretly is far beyond our present realization.

Senator KENNEDY. That is an extremely helpful commentary, and it has been most informative for us to hear you recall the history and the development of the present situation as you see it.

What about the argument that we ought to tap and bug foreign delegations because they do it to us? Is that not an argument that is made sometimes?

Mr CLARK. Well, I have heard it from time to time and I find it just an unconscionable position. I thought we stood for something in this country. I thought we believed in justice and freedom and even fairness. Are we so weak and afraid that we can't take care of ourselves if we do not do what others do? I just have no sympathy with the notion.

We have had this mystique of secrecy and it is hard to crack. It is responsible for a major part of the peril of international war that we have today, in my judgment. I would like to see some moral leadership that tells us our strength does not arise from such activities.

I have tried to estimate—I do not know that it is possible—the value of the taps that we have. I know that not 1 percent of the information that is picked up has any possible utility. It would only be an act of extreme carelessness or extreme urgency that would cause the use of a channel that is assumed by reasonable people in the foreign missions in this country to be under surveillance. The purpose is to find out when people are coming or leaving, who they are associating with, what they are talking about and what they are interested in so that you can evaluate with your other sources of information and predict what they may do.

Senator KENNEDY. What would be the impact on our national security if the executive branch were to eliminate all warrentless tapping at the present time?

Mr. CLARK. I think the impact would be absolutely zero. It may seem axiomatic that when you expand the number of people who know a secret, the security of the secret is less. But does adding one to what may be hundreds or thousand have any value? Most of what we legally use this for is to prevent embarrassment, to invade privacy. Is it true that there are just 27 national security taps on today? I cannot tell—the terminology, worries me. Sometimes they say 27 in FBI cases. Unless the definition of FBI cases has changed, 27 would mean there has been an increase. Historically, National Security Council cases, National Security Agency and State Department cases were the great majority. True the FBI serviced these tapes, but they didn't know what they were doing and did not evaluate the information received. They were transmitters. They knew technically how to install and overhear, but the substantive information had no meaning to them. The National Security Agency, the Department of State—if the 27 excludes those and if it excludes teletype machines and things like that, which have always been fairly numerous, why the number is way up. If it includes all wiretaps without court order, the number is down. If the number is down, then it indicates that we did not need even what we had before—at least somebody today believes we did not need what we had before. Watching the effect of pressure on the agencies of questioning them about wiretap, causing them to justify their requests, showed that you could reduce the number substantially without anybody feeling that he was losing anything that had any value more than an old habit.

Senator KENNEDY. How much time does an Attorney General have to review these cases himself, even with the help of an Assistant Attorney General?

Mr. CLARK. Well, you know, that procedure is largely fiction. It is not real. Part of the reason is time, and part is experience. The Attorney General of the United States is a busy person. I do not think any Attorney General, and I have had at least six agree with me, has spent more than 5 percent of his time on the Federal Bureau of Investigation, Federal Bureau of Prisons, Federal Immigration and Naturalization Service, altogether. I do not think an Attorney General really has a background and experience with rare exceptions that would give him any basis for judgment other than hunch. If you really had all the justification that you need, think of the background that you would have to have and the information you would have to have about the different countries that would be involved. If they are domestic groups, my view was and is, and it has now been confirmed by the U.S. Supreme Court that there is no authority to wiretap. There is no inherent power in the Presidency over domestic crime that has not been fully authorized to the Executive by the Congress. The basic police powers are reserved to the States. In foreign affairs, where there is some inherent power arising from the powers that have been specifically delegated in the Constitution, the Executive has a need to know. I think it is a need that is shared with the Congress. The information should be shared with the Congress, with a committee such as this, to determine its reasonableness and with the Foreign Relations Committee, so that the people can have some input through their representative.

It ought to be shared, too, with the agencies involved. Frequently, what I found was that the taps became a source for feeding interesting tidbits or crumbs, you might say, of information to the White House and other agencies from information that had been picked up by the wiretap. If I know, for instance, that a certain ambassador plans to go home the next week and I tell the State Department, they might think I am a pretty smart fellow if they do not remember that I am listening in on phones.

Senator KENNEDY. Does it make any sense to have one rule or procedure for domestic organizations and a different one for foreigners?

Mr. CLARK. Well, I, think that we should have no procedures, because I think we should have no surveillance. But there are inherent differences. There can be no question, in my judgment, that the full play and force of all the provisions of the Constitution apply to our citizens here, probably to permanent resident aliens here, and to activity that arises and occurs entirely in this country, even if it is wholly financed from without. Because we have police power here. We do not have police power in Asia. We thought we did and we found out, or at least we are finding out we do not—we have not found it out yet.

The need for information about foreign military activities can be very great. Even so I think that there is no way that you can justify wiretap under the Constitution, within the country without prior court approval. And I think the Supreme Court will so hold.

Domestic crimes will not be solved by electronic surveillance. Properly used under the fourth amendment, a warrant can issue only when there is probable cause to believe a specific crime has been or is about to be committed and evidence relating to it spoken in a particular room or a specific phone. That will not happen with rare exceptions where police do not already have adequate evidence to arrest. The trouble is that years of wrongful surveillance will occur before the courts so hold and in the meantime, hundreds of people will have their rights infringed, maybe thousands, who knows? Thousands and thousands will be affected because they will believe that they are tapped, and there will be this pall, or this chilling, of free expression, which is protected by the first amendment and so imperative to the discovery of truth and the communication of ideas.

In the domestic area, there must be the most rigid and manifest adherence to all of those provisions of the Constitution. There is an absolute right in the people affected to know. That is fourth amendment law, it always has been fourth amendment law, and it will come to wiretap usage, too.

In the international field, when you are dealing with aliens, we have power to expel them. They have the power to do things within their country that can affect us directly, like nuclear mounting warheads, that we cannot control. The procedures that we need to develop if we are going to continue use of national security tapping are numerous. First we must require prior judicial approval, second a comprehensive executive justification prior to authorization. We can imperil negotiations for instance because one agency might decide it wanted to tap. If it were discovered before or during negotiations you could imagine the effect. It would be reminiscent of the U–2 incident. You can hurt this country by doing a fooolish thing like that. Therefore, you need a full justification by all the interested agencies—not just the Director of the FBI. He does not have background or responsibility in those areas. The Secretary of State and the foreign affairs adviser in the White House need to know and themselves approve any installation.

If the chairman of a committee like this and the chairman of the Foreign Relations Committee do not know, then you do not have knowledge needed to legislate. You need careful review. There are wiretaps that have been on for decades. That is a long time. When you think of the poor people sitting there listening to all that nonsense and waiting for somebody to say something, you ought to wonder whether we have lost our minds. We ought to look at it again and see what we are doing. We should require full evaluations. Every 3 months I required every tap to be reauthorized. That is often enough.

Finally, even in the national security taps, you need a divulgence in time. I do not think the truth hurts. If it does, I would rather be hurt by the truth than by ignorance. So it ought to be told and it should not be 25 years later when it will not embarrass people. It is just something we ought to do.

There ought to be the clearest recognition that once you engage in any surveillance, you risk the possibility of prosecution. That must be clearly understood and expressed. If you are going to put a na-

tional security tap on without a court order, you simply can't consider prosecution and you need to know that you have insulated that information as effectively as human beings can from any possibility that it will leak into prosecution channels. That was the reason that the Assistant Attorney General for Internal Security came to review those things. It did not begin 6 months or a year ago, it began in the later fall of 1966, when I was Acting Attorney General. I wrote Mr. Hoover probably first in October and again in November and finally in December, telling him that I do not know every case in the Internal Security Division, I cannot possibly know every case in the Internal Security Division; I have to rely on somebody else to know every case there. Therefore, I cannot know when he asks me to put a tap on some foreign activity whether it might affect some case we have; therefore, the head of the Internal Security Division needs to know. At that time, J. Walter Yeagley, who was Assistant Attorney General, as he had been with Bob Kennedy, as he had been for Bill Rogers before that and Nick Katzenbach after it, a career man, a man who had been a FBI agent, a man who had spent a professional career in this field, reviewed every one with me.

Senator KENNEDY. What is your feeling about cleansing the government files of the information which the *Keith* opinion has now decided was obtained unlawfully?

Mr. CLARK. All the information should be purged from those files but before anything is destroyed, every individual or organization involved should be advised. It is their right and their business. So if you were Martin Luther King and you had been overheard, I think you ought to be told about it—not just told about it; I think you ought to be given all of the circumstances and the facts—the circumstances under which it happened and then what happened—the tapes and transcripts.

Then if the person overheard wants either the fact or the substance overheard published then the executive branch ought to make it public. I do not think it ought to be made public unless the individual involved says so—because it is his right invaded, has dignity being demeaned. Again it is my guess that most of these so-called domestic taps in the national security field are so outrageous and absurd that the people and the organizations involved would be bemused by it, but perfectly willing to have the material disclosed.

To start destroying the tapes in advance, going through that procedure, is dangerous from a number of standpoints. How do you know it is destroyed? How many memos has the information appeared in without identifying the source?

After the Kent State killings and the unbelievably prejudicial grand jury report—of course, it has been printed in the New York Times and every place else—the court ordered that the grand jury report be destroyed, be burned. That is book burning, in a way. The grand jury report was itself a fact, the fact of failure of the system and of prejudice. You cannot just purge that by burning it. You need to expose it. And it lives on anyway, as does the information that comes from these taps and bugs. The idea that they are held with just a few people knowing it is wrong. It would have no utility if those were the circumstances. If the information is going to be

used, there have to be a lot of people who know about it. And the people who know about it do not include the Attorney General of the United States. He cannot even remember when he approved it, if he did. All he did was spend 5 minutes at the most reading a memo and perhaps making a phonecall to get somebody to come over and explain something to him or answer a few questions. He did not see what was picked up on taps, he does not know that unless somebody bothers to tell him.

Material from taps can be disseminated very widely. So it endures and it finds its way into places that it should never be.

Senator KENNEDY. Why is there such a reluctance to cleanse that material which was obtained unconstitutionally?

Mr. CLARK. I think there are two basic reasons and both are human failures, in a way. One is embarrassment. My judgment is that essentially all of the material that is picked up on taps is only going to embarrass this Government, make it look petty and foolish. Therefore, you do not want anybody to know what it is that you have done who you tapped and what you have overheard.

The second reason is some sense of royal prerogative—you know, I am the king and the king can do no wrong. You have to have confidence in us and, if you knew what I know, you would do what I do—that sort of thing.

Finally, it can be an enormous task. How many documents has the information found its way into?

Senator KENNEDY. How would you characterize the evidence that was presented to you, when you were Attorney General, for warrantless national security devices? Did the authorization requests contain specific evidence of identified threats to national security, or just generalized suspicions that certain types of persons or groups ought to be spied on?

Mr. CLARK. It varied. Generally, if identified the place and person to be overheard and what conversations were expected to be about. As an illustration of the degree of above, there were at least three occasions in which I was requested to put bugs or taps on Martin Luther King, Jr. The last time was April 2, 1968, only several days before he was murdered. Obviously, the request for that authority, which came on a 1- or 2-page memorandum, contained no facts that indicated he was or could have been a menace to this Nation. He was just the opposite. He offered hope for freedom and equality. It contained conclusory language. It said, in part "Communists are joining forces at every turn in treasonous coalition . . . opposing our efforts in Vietnam . . . working with black power advocates to lay foundations for outright guerilla warfare in the streets of our cities." That was pure scare talk. It was all conclusory, without any fact basis.

Senator KENNEDY. Listening to your testimony here this morning about some of your experiences as Attorney General, I gather that you feel that on balance, the intrusion on individual privacy that results from this kind of tapping and bugging far outweighs the benefits to our national interest.

Mr. CLARK. That is right. I could not respect anyone who wanted to wiretap me. I think that applies among nations as well. If we are

going to get along in this world, as we have to do, we simply have to get away from these old ways of surveillance and the mystique of secrecy and try to live openly together. I think we can do it.

Senator KENNEDY. Thank you very much, Mr. Clark. We certainly appreciate your insights and your help.

Our next witness, Mr. Nathan Lewin, was Assistant to the Solicitor General Archibald Cox when Robert Kennedy was Attorney General.

I know Robert Kennedy had a great deal of respect for your legal abilities and for your counsel and judgment. I also know of the high regard John Doar had for your work in the Civil Rights Division. And of course your talents were of great value to Nicholas Katzenbach when you subsequently worked for him at the State Department. You are now a practicing attorney in the District of Columbia after a most distinguished career of public service.

We welcome you.

STATEMENT OF NATHAN LEWIN, FORMER ASSISTANT TO THE SOLICITOR GENERAL OF THE UNITED STATES

Mr. LEWIN. Thank you, Mr. Chairman. I had prepared a rather technical, I suppose, and lengthy statement which, because of the hour and because I will have to be in court at 2 o'clock this afternoon, I would really prefer just to submit for the record and just note that really, the tone and tenor of that statement is directed toward pointing up that if ever the Department of Justice were to seek some amendatory legislation in line with the opinion in the *Keith* case, in line with Justice Powell's suggestion in that opinion, I think it would be very damaging to the national interest if very many of the other protections that are presently included in title III of the Safe Streets Act which have not received much public attention because of the administration's effort to obtain warrantless wiretaps, that these many other protections are in very many ways greater safeguards than even the judicial warrant. I share Mr. Clark's skepticism about the efficacy of judicial warrants alone to prevent rash judgments with regard to tapping.

I also share his view that the most effective way, really, that government can be subjected to public scrutiny and criticism in this are is if they are required to make what they do public, and there are provisions in title III which require that the Department of Justice advise those who are subjects of taps and bugs of the fact that they have been subjected to it, and in fact, allow them civil damage suits if those taps and bugs are not consistent with the act.

I think that those provisions may in the long run, if they are applied to all taps and bugs, prove to be a very effective deterrent.

[Prepared statement follows:]

STATEMENT OF NATHAN LEWIN BEFORE THE SENATE SUBCOMMITTEE ON ADMINISTRATIVE PRACTICE AND PROCEDURE

The Supreme Court's ruling in *United States* v. *United States District Court for the Eastern District of Michigan*, No. 70–153, decided June 19, 1972, rests principally on two legal conclusions. The first resolves a question of statutory

interpretation and the second is a constitutional holding. As a framework for any prepared statement and further discussion, it might be useful to outline these holdings.

First, the Department of Justice has relied, in its defense of warrantless wiretapping and eavesdropping in courts throughout the country, on the language of Section 2511(3) of the United States Criminal Code, which was part of Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Title III, of course, was the portion of the 1968 law which authorized electronic surveillance upon issuance of a judicial warrant. The specific language of the law which the Department of Justice viewed as an authorization of tapping or bugging without a warrant says that no provision in the Act should limit "the constitutional power of the President to take such measures as he deems necessary" for any of five specified purposes related to "national security" (as those terms are broadly used).

The Department of Justice had argued in lower courts that Congress intended by this language to confer on the President (or upon the Attorney General, to whom the President could delegate his power) statutory authority to engage in electronic surveillance for these "national security" purposes even without satisfying the conditions which the law prescribes generally for bugging and tapping. A unanimous Supreme Court, on its examination of the language and history of the provision, held that Section 2511(3) was not intended to expand, contract or even define the President's powers. It was, rather, "a Congressional disclaimer and expression of neutrality." In other words, the Court said that Congress was intending by this provision to say no more than that no implication should be extracted from the Act as to any Congressional policy one way or the other on the constitutional question of "national security" surveillance. And this ruling led the Court naturally into its constitutional discussion.

In the *second* and constitutional portion of its opinion, the Court ruled that the Fourth Amendment's protection against unreasonable and unwarranted searches and seizures prohibits electronic surveillance without prior judicial approval even when the Executive Branch believes that such surveillance is necessary for domestic security. In this part of his opinion, Justice Powell considered and rejected each of the Department of Justice's asserted justifications for unwarranted bugging and tapping in domestic security cases. He noted that "intelligence gathering"—no less than investigation of criminal activity—must be conducted in accordance with the Fourth Amendment, and that "this requires an appropriate prior warrant procedure." (The Justice Department had repeatedly maintained that when it was merely gathering intelligence and not investigating crime, its activities were not to be judged by Fourth Amendment standards.)

In addition, Justice Powell rejected the Justice Department arguments that issues of domestic security are either "too subtle and complex" or too secret to entrust to federal judges. On the first of these claims, he noted that if the threat is so "subtle and complex" that it may not be comprehensible to a judge, the fault may lie with the proof and not with the judge. And on the latter he noted that wiretap warrants were authorized for espionage, sabotage and treason cases—all of which may involve both foreign and domestic security threats.

Expressly left open by the Court's opinion are "the issues which may be involved with respect to activities of foreign powers or their agents." And in closing, Justice Powell also observed that domestic security problems may justify "different standards" than those prescribed for electronic surveillance in the investigation of specific cases covered by Title III of the Safe Streets Act.

Let me turn now to the effects of the decision and what, I suppose, is of particular concern to this body, the implications it has for future legislation.

The first point which, I think, should be made is that even though the Court proceeded through the two steps I outlined above, the second portion of its decision is a square constitutional ruling which cannot be legislatively overruled. In other words, if proponents of warrantless electronic surveillance in the domestic security area were to urge the adoption of a law which expressly provided for the authority which the Justice Department had attempted to read into Section 2511(3), their proposed legislation would be constitutionally invalid under the second portion of the Court's opinion. To be sure, the Court *did* look to see what Congress meant in Section 2511(3), and it spent about

six-and-a-half pages of its opinion analyzing the language and legislative history. But it did so in order to determine whether it was faced with a question of the constitutionality of a statute or simply an issue relating to the constitutionality of an Executive Branch practice which the Congress had neither approved nor disapproved. It found the latter to be true, and it then proceeded to declare the practice constitutionally unsound.

What, precisely, is the scope of the constitutional ruling? At the very least, it is that—except for the "activities of foreign powers or their agents"—the kind of electronic eavesdropping which amounts to a Fourth Amendment search or seizure under *Katz* v. *United States*, 389 U.S. 347 (1967) and *Berger* v. *New York*, 388 U.S. 41 (1967)—that is, unconsented bugging or tapping—may not be conducted by government agents without a "prior judicial judgment" as to the adequacy of the evidence to warrant the infringement on privacy. (There may, of course, be an "emergency" exception of the kind described in Section 2518(7), which authorizes up to 48 hours of unwarranted eavesdropping, although the constitutionality of this provisions has not been authoritatively determined.). It is, in other words, as plainly unconstitutional to tap a man's telephone without a warrant as it is to break into his house and search for evidence without a warrant.

This analogy brings me to a third critical element of the Court's opinion which bears serious consideration by Congress. In the majority opinion joined by six of the eight Justices, the Court was not satisfied to treat domestic security eavesdropping as equivalent to a search or seizure of physical evidence in a routine criminal investigation. Twice in the course of the discussion of the constitutional issue, Justice Powell called attention to the fact that when government officials conduct national security investigations, they jeopardize "constitutionally protected speech" more seriously than the routine investigation of crime. Two sentences in the opinion forcefully summarize this consideration: "Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' "

What must be borne in mind is that the interception of a private telephone conversation—or, indeed, the threat that a private telephone conversation may be overheard by a government agent—is an impediment to free speech. And when that private discussion is subjected to an eavesdrop because its participants are "unorthodox" in their political beliefs, the danger to free speech and political expression is doubly acute. The Court's sensitivity to this risk is manifest from its warning that "private dissent, no less than open public discourse, is essential to our free society." And it behooves Congress, if it ever again deals legislatively with the question of electronic surveillance, to be as aware of these dangers as six members of the Court now are.

Other aspects of the Court's opinion deserve extended discussion. The exception of "activities of foreign powers or their agents" is the most obvious. In a long footnote, the Court's opinion defines the term "domestic organization" to include one "composed of citizens of the United States . . . which has no significant connection with a foreign power, its agents or agencies." Having rendered this definition, the Court then recognizes that there may be cases where "collaboration in varying degrees between domestic groups or organizations and agents or agencies of foreign powers" may make it difficult to discern on which side of the line an organization falls. How that determination is to be made is left in the air. And, of course, even the basic issue whether warrantless taps or bugs of "foreign organizations" posing a threat to national security are constitutionally permissible has not been decided by the Supreme Court.

Let me turn finally, however, and perhaps most importantly, to the suggestion in Justice Powell's opinion that "protective standards" for domestic security surveillance may be different from the standards which govern the investigation of ordinary crimes. This is an invitation for legislation which the Justice Department may decide to accept. In passing on what that Department may suggest to Congress and what may be offered from other sources, several considerations of both constitutional and practical significance should be kept in mind.

It may be understatement to say that the constitutional principle decided unanimously by the Supreme Court is of tremendous importance. The Court has unequivocally rejected the Justice Department's astounding suggestion that it—that is, the Attorney General—may be both prosecutor and judge of whether private conversations are so likely to endanger national security that they should be overheard. The duty and responsibility of officials of the Executive Branch, said the Court, "is to enforce the laws, to investigate and to prosecute. But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks." By repeating and reinforcing this principle—which, until the Justice Department's novel suggestion in the "national security" wiretap cases, had been taken for granted by constitutional experts—the Court performed a great service for (in Justice Powell's words) "the people of our country."

Important as may be the principle that a government official wishing to tap a phone or bug a room may not do so on his own, it is only as effective in practice as the judicial authority which stands between him and the private conversation he wants to overhear. In the final analysis, the proceeding which even under the Court's ruling, must precede the tap or the bug is an *ex parte* proceeding. The government agent provides an affidavit to a judge in chambers, and the judge, without hearing any evidence or legal challenge on the other side and possibly without doing more than giving the papers a cursory glance, decides whether to issue the warrant. In 90 cases out of 100 under Title III of the 1968 Act, judges have issued warrants on request of federal officials. There have been years, in fact, when the government's batting average was 1.000.

I do not totally discount the possibility that the Justice Department puts those investigations which call for electronic eavesdropping so perfectly in order that its requests for warrants are always—or virtually always—proper in content and form. The fact that some reported cases have found wiretap orders invalid (*e.g.*, *United States* v. *Eastman*, 326 F. Supp. 1038[M.D.Pa. 1971]) and overboard (*United States* v. *Vega*, 52 F.D.R. 503 [E.D.N.Y. 1971]), and that a substantial defect in the Justice Department's authorization procedure has been uncovered (*e.g.*, *United States* v. *Focarile*, 11 Crim. L. Rep. 2008 [D. Md. 1972]; *United States* v. *Robinson*, 40 U.S. Law Week 2454 [5th Cir. 1972]) tends to show, however, that not all is as perfect as it may seem from the statistics of success. And my own experience of six years in three Divisions of the Department of Justice—one of which oversees the work of most of the others—makes me skeptical of any such possibility. I saw far too many cases of inadequately drawn search and arrest warrants—even in notorious cases where time and effort were not spared—to believe that suddenly eavesdropping warrants are immune from the viruses of sloppiness and inefficiency which occasionally strike civil servants.

The danger that a Justice Department eavesdropping warrant application may be routinely rubber-stamped by a sympathetic judge is accentuated, of course, not only by the *ex parte* nature of the proceeding but also by the government's ability to choose its judge. In most every district there are judges who will, in such an uncontested proceeding, routinely give the government what it wants. And so the Supreme Court's rule that there must be an "independent check upon executive discretion" is likely to be more important in principle than effective in practice.

It is my opinion—and I offer it as such—that far more effective practical checks on unbridled electronic surveillance are the less well-known provisions of Title III. Specifically, I refer to the requirements of Section 2518(8), which direct that recordings be kept of all intercepted conversations and that they be maintained under seal for ten years, and that within 90 days of the termination of a surveillance the subject of the surveillance be served with an inventory of the overhearing. These retention and service requirements, as well as the time limitation prescribed by Section 2518(5)—which authorizes an initial 30-day interception period and not more than one 30-day extension—act as a substantial restraint. How effective they are can be seen by comparing the practices which the Justice Department has followed to date in its "national security" investigations (where it has not viewed itself as being bound by the provisions of Title III) with those in Title III cases. Uniformly, recordings of "domestic security" wiretaps have been erased "in the ordinary course of busi-

ness." Uniformly, subjects of "domestic security" surveillance have not been told, even after the taps or bugs were removed, that they had been subject to eavesdropping orders. And, as recent correspondence between the Chairman of the Subcommittee and the Department of Justice has disclosed, security wiretaps and bugs have been continued for longer than the 30 or 60-day periods envisioned by Title III.

So long as the Department of Justice must file, with a federal court, albeit under seal, a complete recording of its wiretap, so long as the duration of a bug or tap is limited in time, so long as it must be disclosed, after that limited time, to the subject of the surveillance, substantial external checks—possibly more effective than a judge's hurried review of its papers—are protecting the public against rash judgments. And this is particularly true when these provisions are reinforced by the civil damage remedy of Section 2520 (so that an individual who is notified of an eavesdrop may sue for damages) and by the direction in Section 2518(5) that a surveillance must "be executed as soon as practicable" and must "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter," and when the affidavit supporting the application must specify why "other investigative procedures" cannot be used. If these peripheral safeguards were wiped away, the judicial warrant requirement would, I believe, be protective in shadow, but not in substance.

Justice Powell's opinion suggested three areas in which Congress might provide "different standards" for "national security" warrants than for others. The first two relate to the nature of the application and affidavit and to the court to which the application should be directed. The third area—which I view as far more critical—relates to "the time and reporting requirements" of Section 2518. I would strongly urge that if, in fact, amendatory legislation is considered—and even that step should not be taken unless the Justice Department demonstrates a strong need for amendment—no exception be permitted from the important provisions of Section 2518 for any kind of electronic surveillance.

Senator KENNEDY. You were here during Mr. Maroney's testimony about how the Justice Department will interpret the *Keith* opinion. Do you have any comments you would like to make about that interpretation?

Mr. LEWIN. There were two aspects of Mr. Maroney's testimony which I thought were encouraging and of course, very many which I thought were distressing.

The two that I though were encouraging were first, that the Department, apparently, will not claim any authority to conduct any wiretaps in the domestic area other than pursuant to title III. That had not been clear from the Attorney General's statement after the *Keith* case, and I think there had been some concern as to whether they might seek to devise some means of obtaining some judicial approval, but still not meeting the title III requirement. So I think that has been clarified, and I think to the good.

The second encouraging remark that Mr. Maroney made was that they are not looking for any amendatory legislation, therefore they are not going to be taking up Justice Powell's interpretation that they seek different standards for domestic wiretaps. Essentially, what he has said, I think, what the Government has in effect confessed by withdrawing those six wiretaps and making no proposal for amendatory legislation is that those wiretaps were not essential to the national security. Apparently, the Government is prepared to go ahead and there is no threat to our national security because on June 20, they were removed, and they are not going to reinstall them. Nor are they going to look for legislation under which they would be able to reinstall them. So those two aspects of his testimony I think are encouraging.

The most discouraging aspect, I think, is the numbers game. The representations are again made that there are only six that had to be removed as a result of this opinion and that there are 27 that are still in effect. One can't conceive that there are 27 foreign embassies engaged in the kind of conduct that Mr. Clark was referring to or likely to be engaged in the kind of conduct or kind of discussions on the telephone that he was referring to that require wiretaps today. So that means that there are many taps in effect that, even if they are, within the Department of Justice standards, not domestic organizations, are of very dubious legality and morality.

In addition, there are one or two domestic organizations which are still being tapped because of some alleged connection to some foreign power and that infringes very seriously on the very first and fourth amendment rights which Justice Powell eloquently referred to, which I know that you, Mr. Chairman, quoted earlier in the hearings today.

I am also concerned that the Department of Justice does not see the obligation which Mr. Clark referred to and which I think is just terribly important, too, now that their conduct has been declared unlawful, to advise those against whom it has acted as to what it has done. When you asked them about cleansing their records, Mr. Maroney's response was that there may be criminal defendants at some time in the future who may move and, therefore, those records will be produced. It would seem to me that in the light of the Supreme Court decision, it is the obligation of the Attorney General today, not later than today, to turn to every single organization and person who has been subjected to an unconstitutional bug or wiretap and say to him, here is the time, here is the place, here is the basis upon which we did it and Congress has given you a civil right of action against me or against my predecessor, against Mr. Mitchell, which you can test in the courts.

The Government, the Department of Justice, is in fact now the respository, the sole repository, of facts upon which the rights of probably thousands of Americans turn. And they apparently have no intention of ever disencumbering themselves or disgorging those facts or producing them to the people whom they have wronged.

So those, I think, are several areas that trouble me. And certainly, the implicit representation in Mr. Maroney's testimony that they view the *Keith* case, the reservation of the power regarding the authority of the Department of Justice regarding the foreign organizations, as being a green light to continue what they have done heretofore—that is troublesome. I think they should recognize that even foreign organizations and members of foreign organizations have first amendment rights. I think Mr. Maroney said, well, there are no first amendment rights involved in the foreign area. That is just not true. Certainly, our courts would recognize the rights of aliens who are within this country, who are on these shores, to express themselves, to speak privately and publicly. And in fact, the Department of Justice has denied that to this committee this morning.

Senator KENNEDY. Do you have any views about the future direction of the court's rulings in this area?

Mr. LEWIN. I think the greatest surprise, Mr. Chairman, to both strong opponents and proponents of wiretapping and bugging in national security cases was the fact that the Court decided this case 8 to 0, unanimously, with not a single vote supporting the Government's position. I think it is a demonstration that in the future, when it is confronted with cases of this kind, where the issue is presented, although not squarely the same issue here, but related areas, as to whether the executive branch may act entirely on its own, without any judicial oversight, without any safeguards, without any restrictions, it will strike that down. And it will strike it down because I think the Court recognizes, no matter who is on that Court, no matter what the political tenor or affiliation or even prior views of the members of that Court are, that in the last analysis, rights of citizens and indeed, rights of aliens, can't be made to turn solely on the unbridled discretion of people who are in the business of prosecuting cases. That just can't be done.

The interesting thing, I think, about this case, too, is that the author of the opinion, Justice Powell, as a private citizen had written an article that received substantial publicity and that was at odds with what he wrote as a Justice. I think it demonstrates that the Court as an institution and the members of that Court recognize that they have to protect the rights of American citizens and indeed of aliens, too.

Senator KENNEDY. Do you think that the Justice Department ought to be applying this decision in its most narrow terms, or do you believe they have a responsibility to try to clarify the law in this area?

Mr. LEWIN. I certainly think they have an obligation to pick up the language which is strictly unnecessary, in the Court's opinion, the language regarding the first and fourth amendments, and say that really, that is a message to the Department of Justice—whether it would be to the Solicitor General, to the Attorney General, to the entire Department of Justice—that the Court is saying that when you actually deal with speech, when you deal with conversations, you are not dealing with contraband, with drugs, with guns. When you are intercepting somebody's conversation, you are entrenching on a constitutionally protected area and that what the Supreme Court has told the Government is that you can never do that, whether it is in the domestic area or in the foreign area, entirely on your own. So I think they do have an independent obligation to carry forward.

And indeed, I would think, from the point of view of the Congress, even if the Justice Department is not picking up Justice Powell's invitation, on the other side the Congress may find it desirable to enact a statute specifically prohibiting foreign power wiretaps without judicial oversight. It appears now as if the Department of Justice intends to continue to pursue its practice that is followed heretofore of engaging in foreign power wiretaps without any judicial warrant.

Now, Mr. Clark this morning, I think, has really stated quite a workable standard for judicial warrants, which is that if the evidence shows that there is a direct and significant effect upon the for-

eign government's power to commit violence upon the United States, then there might be a basis for issuing a judicial warrant. I do not see why that cannot be put into title III prohibiting all—all—wiretapping or eavesdropping even of foreign organizations unless a judge is satisfied from a warrant that that standard is met. And as he explained the materials that were submitted to him as Attorney General, they are certainly within the understanding, within the grasp, within the timeframe that a district judge can apply to that kind of a case.

Senator KENNEDY. Of course, if the Justice Department is wrong in its interpretation, there may be 2 or 3 more years of unconstitu- respoitory, the sole repository, of facts upon which the rights of tional tapping.

Mr. LEWIN. I wish it were only 2 or 3 more years. I think the problem is that the Justice Department intends to continue and that cases in the foreign area, Mr. Chairman—I think what must be borne in mind is that in the foreign policy area, in most of this tapping and bugging, most of it never becomes public and will never become public under the Department of Justice policy announced today, because it does not result in any prosecution. And if it does not result in any prosecution, there may be 3 or 4 years before there is ever a case which even remotely raises the issue of a foreign organization wiretap. That is when the case may first come up in the district court, and by the time it gets up to the Supreme Court, it could be 6 or 7 and there could be thousands upon thousands of people affected.

Senator KENNEDY. A very helpful statement and a very thoughtful commentary. Your testimony will be a very valuable addition to our understanding of this subject.

We want to thank you very much for coming. I hope you get to court on time.

The subcommittee stands in recess, subject to the call of the Chair.

[Whereupon, at 1:30 p.m., the subcommittee was adjourned, subject to the call of the Chair.]

Additional Exhibits

TEXT OF LETTER BY SENATOR EDWARD M. KENNEDY, CHAIRMAN, TO MEMBERS OF ADMINISTRATIVE PRACTICE SUBCOMMITTEE REGARDING NON-COURT ORDERED ELECTRONIC SURVEILLANCE

DECEMBER 17, 1971.

DEAR SENATOR: As you may have noticed in two recent speeches and at Judiciary Committee hearings a few weeks ago, I referred to the fact that there has been three to nine times as much federal listening going on as a result of warrentless electronic surveillances as there has been on devices operated under judicial authorization.

Some of the members of the Subcommittee have asked for the factual data underlying my statements on this subject, and I thought I would take this occasion to forward to all of the members copies of the correspondence I have had with the Justice Department which gave rise to these observations. I would also like to share with you some other preliminary conclusions I have reached about issues raised in this correspondence in keeping with the significant oversight this Subcommittee has exercised with respect to the subject of electronic surveillance in the past.

Briefly stated, study of the correspondence and related public materials suggest that: 1) the number of federal wiretapping and bugging devices installed without court authorization is substantially greater than the Executive Branch has led the public to believe; 2) the average duration of such devices is many times longer than the average duration of court-approved devices; 3) as a result, the total amount of federal electronic eavesdropping without court permission far exceeds the eavesdropping with judicial approval; 4) there is strong reason to doubt the validity of the repeated public assurances by the Justice Department that it fully complies with the 1968 Congressional standards before installing any tap or bug without a court order; and 5) despite the Department's assertions to the contrary there is an absence of well-defined procedures which would promote compliance with the statutory standards and permit meaningful Congressional scrutiny of this extraordinary Executive activity.

I am sure you are aware of the fact that numerous public statements have been made by high federal officials during the past year suggesting that there is a comparatively limited amount of federal electronic surveillance operated without court orders.

For example in April President Nixon told the annual convention of the American Society of Newspaper Editors:

> Now in the 2 years that we have been in office—now get this number—the total number of taps for national security purposes by the FBI, and I know because I look not at the information but at the decisions that are made—the total number of taps is less, has been less, than 50 a year.

And, just three months ago the Solicitor General told the Supreme Court in a brief filed in the *Keith* case (the case still pending on the constitutionality of warrantless electronic surveillance) that only 36 warrantless telephone surveillances were operated in 1970.

The above figures are flatly contradicted by Assistant Attorney General Mardian's March 1 letter to me, in which he reveals that a total of 97 warrantless telephone taps were operated in 1970—almost double the President's figure, and almost triple the Solicitor General's figure. (This ratio excludes the 16 microphone installations in 1970, which neither the President nor the Solicitor General took note of.)

Further, the repeated references by Government officials to the limited number of warrantless devices ignore the far more significant question of the duration and total usage of these surveillances. I am extremely concerned about the fact that in 1970 there were from 3.4 to 9.6 times as many days of

federal listening on warrantless devices as there were on devices installed under judicial authorization. To assist you in your assessment of this problem I am attaching a chart which reflects the figures upon which these ratios are based. You will note that the calculations we have made also reflect that for the two-year period 1969–1970, warrantless devices accounted for an average of 78 to 209 days of listening per device, as compared with a 13-day per device average for those devices installed under court order.*

In short, Mr. Mardian's March 1 reply poses the frightening possibility that the conversations of untold thousands of citizens of this country are being monitored on secret devices which no judge has authorized and which may remain in operation for months and perhaps years at a time. The figures certainly seem to suggest that the Attorney General was being less than accurate last April when he said on the David Frost Show that these Executive-ordered devices "relate to particular subject matters at a particular time", if he meant to imply that such devices were installed only briefly and only to enable the Government to prevent specific acts threatening immediate peril to the security of the nation.

Apart from the indication that these surveillances are apparently far more pervasive than any of us had ever realized, the correspondence raises the recurring problem of whether any standards and guidelines are being followed in the employment of these techniques. As you will recall, in enacting the Safe Streets Act of 1968, Congress described five categories of danger to the Nation for which warrantless devices might be utilized if they were constitutionally permissible at all namely: (1) to protect the Nation against actual or potential attack or other hostile acts of a foreign power; (2) to obtain foreign intelligence information; (3) to protect national security information against foreign intelligence activities; (4) to protect against the overthrow of the government by force or other unlawful means and (5) to protect against other clear and present danger to the structure or existence of Government. Of course, there is a substantial issue, now before the Supreme Court, as to whether any such warrantless electronic surveillances are permissible under the Fourth Amendment, but on the assumption that some are, the Justice Department has repeatedly assured the courts that it is operating under procedures and standards which assure strict control and complete adherence to the statutory categories.

For example, briefs and memoranda filed by the Department in several cases in support of this claim that warrantless electronic surveillances are lawful contain the following unequivocal assertions:

"Another restraint on the exercise of the power is the existence of strict standards, recognized by the Congress which are met before the President or the Attorney General acts. . . . Additionally, there exists a compelling wisdom in the policy of having one official, the Attorney General acting for the President, to authorize such a surveillance in accordance with the standards set forth in the Omnibus Crime Control and Safe Streets Act of 1968, in order that such policy will provide a uniformity in the application of those standards. . . ." [See, e.g. Memorandum in *U.S.* v. *Bieber*, 71 CR. 479, E.D.N.Y.]

Indeed, the Solicitor General's most recent brief on the subject, which was filed in the Supreme Court in the *Keith* case just three months ago, contained the assurance that:

"The standard of the national security that the Attorney General applies in authorizing electronic surveillance without a warrant is the same standard that Congress provided in the Omnibus Crime Control and Safe Streets Act of 1968."

The brief then refers to the five statutory categories described above and says: "three of these categories relate to the hostile acts of a foreign power and to foreign intelligence activities and are not directly involved here." It continues: "The two other categories are 'to protect the United States against the overthrow of the Government by force or violence or by other unlawful means, or against any other clear and present danger to the structure or existence of Government,'" citing the 1968 statute. It concludes: "These were the grounds upon which the Attorney General authorized the surveillance in the present case."

---

*Duration figures for noncourt ordered devices are given in terms of maximum and minimum levels because the information provided is in terms of duration ranges. See pages 1, 2, 3 of March 1 letter.

Obviously this officially asserted Executive compliance with Congressional standards is vital in an activity which lies in the grayest possible area of Constitutional law. Certainly Congress expected that well-defined procedures would be established to guarantee that each warrantless surveillance would clearly meet one or more of those categories when installed, and the public has the right to assume that these limits on electronic surveillance are being assiduously applied in every instance. Moreover, precise prior categorization of such surveillances is necessarily central to Congressional review of the implementation of the 1968 law, and is essential to a full understanding of the overall figures, discussed above, relating to the amount and duration of bugging and tapping on the sole discretion of the Executive Branch. For example, if it were true that 95% of the total number of installations were initiated for the sole purpose of obtaining foreign intelligence information from aliens, and only 5% for the purpose of surveilling domestic dissidents whom the Attorney General genuinely considered to be a clear and present danger to the existence of the Government, the meaning of the statistics might be quite different from the meaning if the percentages were reversed. Indeed, if the "clear and present danger" category were being used at all regularly, the Congress would certainly want to hear more about the nature of that danger.

It was with these considerations in mind that my original letter asked the Attorney General to provide a breakdown of the Executive-ordered surveillances by statutory category. I was therefore disappointed when Mr. Mardian's first reply failed to provide such a breakdown, allegedly because the "installations cannot be categorized exclusively under a single criterion," although he did assure me that each installation met one or more of the statutory criteria.

I thereupon indicated that the breakdown could be made in terms of more than one category. This time I was surprised and dismayed to receive a response which said not only that the subject matter "is such as to preclude categorization under a single criterion, "but also that "no such categorization exists."

I next requested merely that the Department provide the number of installations which fell into either of the categories which the Department itself had spelled out in its court submissions, namely those employed to gather "foreign intelligence information" and those employed to gather "intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of Government," the latter of which, I should point out, is *not* one of the statutory categories. Mr. Mardian's response to this request was absolutely shocking, in view of the position of the Department in the Courts. "The Department," he said, "has never attempted such a categorization."

Thus, despite the litigative positions taken by the Department and the assurance by Mr. Mardian, in his March 1 letter to me, that the Attorney General's discretionary wiretaps and bugs all fall within the statutory categories, the Department now admits in essence that it actually does not know—and thus presumably does not care—which installations fall into which categories. It seems clear from the correspondence that when the Attorney General is asked to authorize a warrantless electronic surveillance, he is not told what category or categories justify its use, nor how the statutory elements for the category or categories are met by specific facts; for if he were, the Department would have had no difficulty at all providing the statistical breakdown I requested.

This conclusion is strengthened by the Department's response to my effort to determine the precise nature "of the administrative practices and procedures which culminate in a determination whether [the statutory] criteria have been met." In court, of course the Department has consistently asserted that in applying the statutory categories, "there exist adequate procedures to insure that the standards are met." (See, e.g. Memorandum in *U.S.* v. *Hoffman*, CR. No. 973–71, D.C.) But in his answer to my inquiry, Mr. Mardian, on behalf of the Attorney General, was "unable to supply" any information on those procedures, other than to say that applications for electronic surveillances to be ordered by the Attorney General "have come from the Director of the Federal Bureau of Investigation personally," and "are handled exclusively by the Attorney General acting for the President."

Apart from the fairly explicit admission, once again, that there really are no procedures to assure adherence in advance to the statutory standards, the response raises new questions of who is doing what and why. For in June, on

the one hand the Attorney General, in a speech in Roanoke, Virginia, was stating flatly that "only the President is in a position to evaluate adequately" the kinds of sensitive information relevant to so-called "national security" surveillances, because only the President is familiar with "the various intelligence data submitted by the independent agencies within the intelligence community." On the other hand, the Deputy Attorney General the same month was arguing (on the Liz Drew Show) that the requisite judgements should be made in the Executive Branch because of the presence there of "professional career people" who "understand" sensitive materials. Yet if Mr. Mardian's response is accurate, it is neither Presidential expertise nor career expertise that is being applied but the lone judgement of the Attorney General based on each separate submission to him by the investigators who wish to do the surveilling, and without specific focus on the statutory criteria.

The answer to this seeming inconsistency, and to other issues raised in the correspondence, such as whether federal dissemination of information from warrantless taps and bugs—not identified as such—to state law enforcement agencies may be tainting many local cases across the nation, will have to await the Subcommittee's further pursuit of these matters next year, but I wanted to bring you up to date in view of the inquiries from some Subcommittee members, as well as from the academic and legal communities and the press.

At the very least, the correspondence demonstrates that any reliance on Congressional scrutiny as a continuing constraint on Executive abuse of "national security" eavesdropping is misplaced. The Deputy Attorney General has specifically suggested (on the Liz Drew Show) that "Congress . . . is informed regularly" with respect to the "categories" of such surveillance. According to the Department's brief *in Keith* placing sole responsibility in the Attorney General permits greater control over use of this technique by facilitating close Congressional oversight of the Executive's action." The correspondence, however, shows plainly that the Department has no procedures or record-keeping practices which allow, let alone facilitate, any meaningful Congressional review of the purposes for which warrantless taps and bugs are being used, or the way in which the statutory criteria are being met.

The copy of the correspondence I am enclosing is unedited, but the Justice Department has requested that the specific surveillance duration figures not be released, and the copies made publicly available will have those figures excised. I believe that you will find the enclosed chart, which is derived from these figures but does not disclose them, adequate for any public discussion of this material.

I look forward to working with you on these and other subjects of mutual interest during the coming year, and I thank you for your assistance and participation during 1971.

With best holiday wishes.

Sincerely,

EDWARD M. KENNEDY,
Chairman, Subcommittee on Administrative Practice and Procedure.

FEDERAL WIRETAPPING AND BUGGING, 1969–70

	Court ordered devices		Executive ordered devices			Ratio of days used: Executive ordered, court ordered		Average days in use per device		
				Days in use				Court ordered devices	Executive ordered devices	
	Number	Days in use	Number	Minimum (rounded)	Maximum (rounded)	Minimum	Maximum		Minimum	Maximum
1969	30	462	94	8,100	20,800	[1] 17.5	[1] 45.0	15.4	86.2	221.3
1970	180	2,363	113	8,100	22,600	3.4	9.6	13.1	71.7	200.0
Total	210	2,825	207	16,200	43,400	5.7	15.4	13.5	78.3	209.7

[1] Ratios for 1969 are less meaningful than those for 1970, since court-ordered surveillance program was in its initial stage in 1969.

Source: (1) Letter from Assistant Attorney General Robert Mardian to Senator Edward M. Kennedy, Mar. 1, 1971. Source figures withheld at request of Justice Department.
(2) 1969 and 1970 reports of Administrative Office of the U.S. Courts.

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C., February 5, 1971.

Hon. JOHN MITCHELL,
Office of the Attorney General,
Department of Justice,
Washington, D.C.

DEAR MR. ATTORNEY GENERAL: As you know, the Subcommittee on Administrative Practice and Procedure has in recent years been extremely interested in the subject of electronic surveillance, both in connection with its continuing study of practices of federal agencies and others that may constitute invasions of privacy and its role in the development and processing of the legislation which eventually became Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Both of your immediate predecessors and other Department officials appeared before the Subcommittee and their assistance was extremely valuable in our work. I know that your knowledge and interest in this area will also prove helpful to us, and we look forward to working closely with you and your staff.

There has been increasing concern in the Congress and in the Nation in regard to the current practices of the Federal government in the utilization of electronic surveillance. You yourself have announced a six-fold rise in the number of court-ordered wiretaps and microphone eavesdrop installations between calendar 1969 and calendar 1970, and there have been a growing number of court cases involving surveillances initiated by the Federal government without court orders. You have offered detailed and impressive defenses of the increase in installations under court order, and, of course, we will be assisted in reaching our own conclusions as to that type by the annual reports of the Department on its applications to the courts for wiretap and eavesdrop orders.

In the case of electronic surveillance installations made without court orders, the public impression is that such installations are not only being made more frequently, but also that they are being used in a growing spectrum of types of cases. Many citizens fear that installations without court order are being used to avoid the requirements governing court-ordered installations, and especially the necessity for the government to prove probable cause as to commission of specified criminal offenses to obtain a court order. They reason that if there were facts to establish that such criminal offenses were involved in a given case, the government would proceed by court order, and that the increasing avoidance of this procedure reflects increasing surveillance of individuals and groups whose only offense is disagreement with government policies, personal eccentricity, outspokenness, or participation in lawful activities of organized dissent, or a combination of these.

The problem for those of us who must assess these concerns is that in the field of purely executive wiretapping and eavesdropping, as opposed to Executive tapping and bugging under Judicial authority, we have scant information on which to base our judgments. The Director of the Federal Bureau of Investigation has annually testified as to the number of "national security" installations, and other Department officials including the Attorney General have from time to time also referred to such a figure in Congressional testimony or correspondence. I believe that the most recent such report referred to 36 wiretaps and 2 microphones.

In view of your own statements as to the increased number of non-court-ordered installations, the growing public concern, the need of the Congress and the public for more information from which to determine whether and how the limitations on such installations in Section 2511(3) of Title III are being adhered to, Constitutional questions aside, I am confident that you will agree that this would be an opportune time to shed some light on Federal practices in this area.

Would you, therefore, kindly provide the following information as soon as possible, sending us immediately those items of information which are readily available, and the remainder when obtained. I recognize the fact that some of

the statistics requested will be based on documents which are classified, but the requests have been phrased so as to admit of answers which should be able to be unclassified. However, if you see a need to classify any particular answer, please provide it separately, and it will be handled on a classified basis.

A. For the period June 19, 1968 to December 31, 1968, for calendar 1969, and for calendar 1970, please provide:

1. The number of electronic surveillance installations placed in operation or continuing in operation at any time during the period, counting each device, connection, or other unit as a separate installation where more than one installation was utilized to surveil the same subject or group of subjects.

2. Of these, for each period, the number of each type of installation, i.e. wire communication intercepts, oral communication intercepts, combination intercepts, or other.

3. For each period, the number of installations in each of the following time categories: under 1 week, 1 week to 1 month, 1 month to six months, over six months.

4. For each period, the number of installations in each use category itemized in Section 2511(3) of Title 18, U.S. Code, as added by Title III of P.L. 90-351, i.e.

a. to protect the Nation against actual or potential attack or other hostile acts of a foreign power,

b. to obtain foreign intelligence information,

c. to protect national security information against foreign intelligence activities,

d. to protect against the overthrow of the government by force or other unlawful means,

e. to protect against other clear and present danger to the structure or existence of government (for this category, describe general nature of danger).

5. For each period, the number of installations the dissemination of whose product fell in each of the following categories:

a. disseminated only to 5 or fewer persons within the Federal government,

b. disseminated only to 5 to 50 persons within the Federal government,

c. disseminated to over 50 persons in the Federal government only.

d. dissemination total unknown but available on request to properly cleared Federal employees only.

e. disseminated to state, local, or private agencies.

B. In the light of the recent conflicts among the Federal courts as to the Constitutional and statutory limits of the government's power to initiate electronic surveillance without judicial authority, what interim standards and procedures has the Department adopted pending ultimate determination of these limits on a nation-wide basis?

I appreciate your assistance and look forward to your reply.

Sincerely

EDWARD M. KENNEDY
Chairman, Subcommittee on Administrative Practice and Procedure.

DEPARTMENT OF JUSTICE,
Washington, March 1, 1971.

HON. EDWARD M. KENNEDY,
Chairman, Subcommittee on Administrative Practice and Procedure,
U.S. Senate.
Washington, D.C.

DEAR MR. CHAIRMAN: The Attorney General has asked me to respond to your inquiry of February 5, 1971, with respect to administrative practices and procedures relative to electronic surveillance.

In accordance with your suggestion, we would ask that the breakdowns furnished with respect to the duration of surveillance be treated as confidential since an examination of the breakdown might indicate a fixed number of permanent surveillances.

With respect to your questions A1, A2, and A3, we submit the following:

June 19 to December 31, 1968

Telephone surveillances:
- In operation less than one week.
- In operation 1 week to 1 month.
- In operation 1 to 6 months.
- In operation more than 6 months.

Total, 50

Microphone Surveillances:
- In operation less than one week.
- In operation 1 week to 1 month.
- In operation 1 to 6 months.
- In operation more than 6 months.

Total, 6

Calendar Year 1969

Telephone Surveillances:
- In operation less than one week.
- In operation 1 week to 1 month.
- In operation 1 to 6 months.
- In operation more than 6 months.

Total, 81

Microphone Surveillances:
- In operation less than one week.
- In operation 1 week to 1 month.
- In operation 1 to 6 months.
- In operation more than 6 months.

Total, 13

Calendar Year 1970

Telephone Surveillances:
- In operation less than one week.
- In operation 1 week to 1 month.
- In operation 1 to 6 months.
- In operation more than 6 months.

Total, 97

Microphone Surveillances:
- In operation less than one week.
- In operation 1 week to 1 month.
- In operation 1 to 6 months.
- In operation more than 6 months.

Total, 16

The annual totals set forth above can be misleading in that they reflect the total installations authorized or in place during the periods described. The total maximum number of surveillances in operation at any one time during the periods described are as follows:

June 19 to December 31, 1968	
Telephone surveillances	45
Microphone surveillances	6
Calendar Year 1969	
Telephone surveillances	59
Microphone surveillances	5
Calendar Year 1970	
Telephone surveillances	56
Microphone surveillances	6

With respect to your question A4, the installations cannot be categorized exclusively under a single criterion; however, each installation meets one or more of the criteria itemized in Section 2511(3) under Title 18 of the United States Code.

Departmental records do not, as a practical matter, permit us to answer question A5 with the specificity you request. However, Department policy limits dissemination of information of the nature inquired of to persons on an actual "need to know" basis. Appropriate security classifications and control markings are imposed on such information. None of this information is disseminated to state or local governments or agencies except in rare instances in order to prevent the commission of a serious felonious act. In such instances, the source of the information is not divulged.

In response to question B, we would advise that since the *Katz* decision in 1967, the Department has operated under the more restrictive guidelines dictated by that decision and the standards enunciated in the Omnibus Crime Control and Safe Streets Act of 1968, which codified the parameters of the "national security" exception. No changes in Department practices or procedures have been initiated by reason of the conflict in the recent district court decisions to which you refer.

Sincerely yours,

ROBERT C. MARDIAN,
Assistant Attorney General.

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C. March 12, 1971.

MR. ROBERT C. MARDIAN,
Assistant Attorney General,
Department of Justice,
Washington, D.C.

DEAR MR. MARDIAN: Thank you for your letter of March 1 replying to some of my inquiries relating to electronic surveillance.

Although I can appreciate that each of the surveillances operated without court order may not necessarily be susceptible of categorization exclusively under any single criterion enumerated in Section 2511 (3) of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, we would nevertheless like to have a numerical break-down by category or categories of the installations described in your letter. In this regard, we would also appreciate your supplying us with a detailed description of the administrative practices and procedures of your Department which culminate in a determination whether Section 2511 (3) criteria have been met and whether a recommended surveillance should be approved.

I appreciate your assistance.

Sincerely,

EDWARD M. KENNEDY.

DEPARTMENT OF JUSTICE,
Washington, March 23, 1971.

Hon. EDWARD M. KENNEDY
Chairman, Subcommittee on Administrative Practice and Procedure,
U.S. Senate,
Washington, D.C.

DEAR MR. CHAIRMAN: As indicated to you in my letter of March 1, 1971, the subject matter of question A–4 is such as to preclude categorization under a single criterion and no such categorization exists.

I am unable to supply you with a "detailed description of the administrative practices and procedures" you request, other than to say that all requests for telephonic and microphonic surveillances, at least since January 20, 1969, to the Attorney General have come from the Director of the Federal Bureau of Investigation peronally. Such requests are handled exclusively by the Attorney General acting for the President of the United States.

This Department has heretofore publicly set forth the considerations involved in making such determinations and the reasons for refusing to disclose the bases for the Executive's decision. In the brief of the United States filed recently in the Ninth Circuit Court of Appeals we said:

"In authorizing the use of electronic surveillance, the President through the Attorney General must weigh many factors, not all of a purely factual nature, which he cannot, and should not be required to, produce before a magistrate. Moreover, in making such a decision the President must rely upon the entire spectrum of information available only to him, much of which is derived from sources which, by their nature, are secret. Such information, more often than not, involves both the Nation's foreign and domestic affairs inextricably intertwined. Any attempt to legally distinguish the impact of foreign affairs matters from internal subversive activities or to isolate one particular factor upon which an eventual decision is based, is an exexcise in futility and eloquently demonstrates the wisdom of leaving these decisions to the Chief Executive who alone is in a position to make such a judgment and who is answerable to the people from whom the power is derived.

"Another weighty factor bearing upon this issue is the fact that disclosure of the bases for the Attorney General's decision or the fact that such a surveillance is to be conducted may in itself prejudice the national interest."

We hope the foregoing will be of assistance to you.

Very truly yours,

ROBERT C. MARDIAN
Assistant Attorney General.

APRIL 1, 1971.

Mr. ROBERT C. MARDIAN,
Assistant Attorney General, Internal Security Division,
Department of Justice,
Washington, D.C.

DEAR MR. MARDIAN: I am writing with reference to your letter of March 23 advising that there is no categorization of the surveillance operated without court order under the criteria enumerated in Section 2511(3) of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

In view of the position taken by your Department in the courts that certain of such surveillances are employed for the purpose of gathering "foreign intelligence information", and that other of such surveillances are employed for the purpose of gathering "intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government", would you please provide us with a numerical break-down of the installations described in your March 1 letter under these two classifications.

I appreciate your assistance.

Sincerely,

EDWARD M. KENNEDY,
Subcommittee on
Administrative Practice and Procedure.

DEPARTMENT OF JUSTICE,
Washington, April 23, 1971.

Hon. EDWARD M. KENNEDY,
Chairman, Subcommittee on Administrative Practice and Procedure,
U.S. Senate,
Washington, D.C.

DEAR MR. CHAIRMAN: This is in response to your most recent letter of April 1, 1971, in which you request a numerical breakdown of those surveillances operated without court order, which are employed for the purpose of gathering "foreign intelligence information" and those which are employed for the purpose of gathering "intelligence information deemed necessary to protect the Nation from attempts of domestic organizations to attack and subvert the existing structure of the government." You indicate that these two categories are derived from the position recently taken in the courts by the Department of Justice.

The position taken by the Department in the courts has drawn a distinction between two separate but closely related powers of the President, pursuant to which he may constitutionally authorize electronic surveillance to gather intelligence information without securing a prior warrant. In the brief of the United States filed recently in the Ninth Circuit Court of Appeals we said:

In *United States* v. *Belmont*, 301 U.S. 324, 328 (1937), the Court recognized the existence and extent of one of these inherent Presidential powers when it held that "the conduct of foreign relations was committed by the Constitution to the political departments of the government, and the propriety of what may be done in the exercise of this power [is] not subject to judicial inquiry or decision." . . . the President, in his dual role as Commander in Chief of the armed forces and Chief Executive, possesses another serious power and responsibility—that of safeguarding the security of the Nation against those who would subvert the Government by unlawful means." (Brief, pages 2–3.)

"As we have indicated, the inherent powers of the Chief Executive to conduct foreign affairs and to protect the national security, while somewhat related, are separate and distinct. The Congress itself recognized the distinction in the Omnibus Crime Control and Safe Streets Act of 1968." (Brief, pages 17–18.)

This position was not intended to imply that any single surveillance could be considered as being employed solely pursuant to either one of the aforementioned powers. As I have indicated previously, the decision to employ such surveillance is based on a consideration of information involving "both the Nation's foreign and domestic affairs inextricably intertwined." Accordingly, the Department has never attempted such a categorization.

We hope the foregoing will be of some assistance.

Sincerely,

ROBERT C. MARIDIAN,
Assistant Attorney General.

DEPARTMENT OF JUSTICE,
Washington, D.C., January 20, 1972.

Hon. EDWARD M. KENNEDY,
U.S. Senate,
Washington, D.C.

DEAR SENATOR KENNEDY: This is in response to your letter of January 19, 1972, inviting me to appear before your Subcommittee on Administrative Practice and Procedure concerning electronic surveillances initiated by the Federal government without court orders.

The Senate Judiciary Subcommittee on Criminal Laws and Procedures, of which you are a member, has been working closely with the Department of Justice in anticipation of a comprehensive examination of all aspects of electronic surveillance. This study has been the subject of correspondence between Senator McClellan and the Attorney General, copies of which were included in the Congressional Record of May 10, 1971 (S 6477-78). As indicated in Senator McClellan's letter of April 28, 1971, the undertaking will include a comprehensive review of law and practice in domestic security cases. We expect to present this material before the Subcommittee in early February.

Our complete analysis is still being prepared. Under these circumstances, it would be premature and inappropriate for me to testify next Tuesday, January 25.

Sincerely,

ROBERT C. MARDIAN,
Assistant Attorney General,
Internal Security Division.

JANUARY 19, 1972.

Mr. ROBERT C. MARDIAN,
Assistant Attorney General,
Department of Justice,
Washington, D.C.

DEAR MR. MARDIAN: This is to confirm the invitation telephoned to you to appear at the hearing of the Subcommittee on Administrative Practice and Procedure on warrantless electronic surveillance on the morning of Tuesday, January 25, 1972, in continuation of our inquiry on that subject which began with my letter of February 5, 1971, to the Attorney General, and with which you have cooperated in further correspondence over the past year.

We would like you to provide the Subcommittee prior to your appearance with copies of any guidelines, instructions, forms, delegations, rules, regulations, or other documents relating to the procedures for requesting, approving, and installing warrantless electronic surveillances, including any materials of agencies or bureaus of your Department or other Departments utilized in connection with requests for the Attorney General's approval of wiretap and microphone surveillance without court order.

Of course, to the extent any specific classified materials or information are involved, the usual precautions and protection will be arranged. And naturally we will not expect you to delve into the specific facts of any pending criminal case. Rather our interst is in the general kind of policy and procedural information which the Attorney General, Deputy Attorney General, and you have discussed in various speeches, interviews, and in your correspondence with us.

I want to stress that we are not at this time considering the provisions of Title III which relate to court-ordered wiretapping in connection with criminal cases, and we would not expect you to be prepared to discuss that area.

Please let me know if the 25th is convenient with you. If another day is preferable we can reschedule the hearing.

With warm regards.

Sincerely,

EDWARD M. KENNEDY,
Chairman,
Subcommittee on Administrative Practice and Procedure.

EXCERPT FROM ADDRESS OF RICHARD G. KLEINDIENST AT BOSTON UNIVERSITY, MAY 7, 1970

* * * * * * *

The other aspect to the wiretap controversy is the non-court authorized electronic surveillance for national security purposes.

Here again, we were faced with constitutional polarities. There are those who believe that every search conducted by government under any circumstances must conform to the Fourth Amendment requirements of a warrant issued by a magistrate.

And there are others who believe that, on the slightest pretext of national security, the Executive should be able to conduct searches free from any court ordered showing of probable cause.

When John Mitchell became Attorney general, he was informed that every Attorney General for the past 25 years had authorized electronic surveillance as a means of gathering foreign intelligence information and intelligence information concerning domestic organizations which pose a serious threat to the national security.

This power has been exercised under the constitutional prerogative of the President to protect the security of the nation upon the belief that the courts would accept the Attorney General's determination that the search was necessary.

Thus, he decided that, as the President's lawyer, it was right and proper for him to defend the actions of his predecessor Attorneys General who acted on behalf of their respective Presidents. We have submitted this matter to the courts for their decision and we will, of course, abide by their rulings.

As a safeguard against abuse, *a complete review* of every existing national security wiretap was instituted. Each application must be presented to the Attorney General personally with full supporting documentation. The result has been a restricted use of non-court authorized electronic surveillance.

* * * * * * *

EXCERPT FROM TESTIMONY OF RICHARD G. KLEINDIENST, FEBRUARY 23, 1972, BEFORE THE SENATE JUDICIARY COMMITTEE

Senator KENNEDY. In the area of wiretapping, Mr. Kleindienst, as you know, the Criminal Laws Subcommittee is going to have some hearings on this matter. Our Administrative Practice Subcommittee has also been interested in this subject in terms of the procedures and practices and rules that have been followed. Our interest follows the rather extensive subcommittee interest which began many years ago under the previous chairman, Senator Edward Long of Missouri. In terms of the categories of warrantless wiretapping, is there really any reason why that kind of information can't be provided to the Congress, such as how many taps are being made under the different categories?

Mr. KLEINDIENST. Categories like microphone and telephone?

Senator KENNEDY. No. In connection with so-called national security taps, such categories for example, "clear and present danger to the structure or existence of government." In the 1968 law there are five different categories for warrantless tapping. What I am interested in is whether you can give us a breakdown as to the number of taps in each of these categories. Is that possible?

Mr. KLEINDIENST. I can't give it to you today. But I see no reason why the number—I know that information has been provided or is provided regularly to the Congress by the Directcor of the FBI.

Senator KENNEDY. I think it would be helpful if we could have it. We do have these different categories, and if we know just the number of devices that were being authorized under each of the different categories, I think it would be useful and helpful.

Senator HRUSKA. Would the Senator yield for a little addition in this regard?

Senator KENNEDY. Surely.

Senator HRUSKA. Mr. Kleindienst, is there any way of estimating how many wiretaps we do not have now by reason of the fact that the present wiretap law makes it illegal for private parties or unauthorized persons to use wiretapping?

Mr. KLEINDIENST. I think as a result of that law, Senator Hruska, there has been a fantastic diminution in electronic surveillances that were instituted by private parties, private snooping.

Senator HRUSKA. How do you know that?

Mr. KLEINDIENST. Well, because most of the people of this country are law-abiding citizens, and when they are advised of the passage of a law by the Congress that carries with it penalties of that kind, I think that they have a natural inclination to comply with the law of the land.

Senator HRUSKA. Would the sale of the equipment that is necessary for this purpose be an indicator in that regard?

Mr. KLEINDIENST. That would be evidentiary.

Senator HRUSKA. What has happened to those sales, and the manufacture of that type of equipment?

Mr. KLEINDIENST. I don't know precisely, but I know it has gone down.

You would also have to take into account that which was already in existence. But I know it has gone down.

Senator HRUSKA. If you could get some estimates in the matter of how helpful this bill has been to really get at unauthorized wiretaps, which had not been illegal before, and also perhaps the volume of manufacture and sales and availability of this type of equipment, it might be helpful to round out the picture.

Mr. KLEINDIENST. That would be interesting information.

Senator HRUSKA. I thank the Senator.

Senator KENNEDY. Has wiretapping ever been legal?

Mr. KLEINDIENST. Well, in national security cases——

Senator KENNEDY. Private wiretapping, the kind of wiretapping you were just talking about?

Mr. KLEINDIENST. Yes——

Senator HRUSKA. It has not been illegal?

Mr. KLEINDIENST. It has not been illegal.

Senator KENNEDY. I thought the Communications Act had made it illegal.

Mr. KLEINDIENST. Well, there are some nice little touchy variations on that. It depends on what you do with it.

Senator KENNEDY. I thought the Communications Act made it illegal.

Mr. KLEINDIENST. Well, there is conduct described in that Communications Act. And if it didn't come within that precise conduct you could go ahead and have the eavesdropping.

Senator HRUSKA. Wasn't this the weak spot in it, it was not illegal to wiretap, but it was illegal to communicate the product of that wiretapping.

Mr. KLEINDIENST. That is correct.

Senator HRUSKA. And so in effect you had a situation where it was not illegal to go ahead and wiretap.

Now, that is no longer the case under the present law?

Mr. KLEINDIENST. That is correct.

Senator KENNEDY. As I understand it on the warrantless wiretap, you make a finding in terms of say, clear and present danger in order to justify such non-court-ordered wiretapping. Do you have any place where there's written down a definition, or an elaboration of what constitutes a clear and present danger?

Mr. KLEINDIENST. Not that I know of, Senator Kennedy, but there might be—this is one function that the Attorney General has never delegated to me in any respect since I have been the Deputy Attorney General.

Senator KENNEDY. So the meaning of these words, "clear and present danger," then, really depends upon your own view, a very subjective kind of a judgment?

Mr. KLEINDIENST. Right.

Senator KENNEDY. Could you give us any kind of idea this afternoon as to the magnitude of that danger, the kind of danger that must be present in order for you to authorize this type of thing? I know it is difficult.

Mr. KLEINDIENST. Those words mean a great deal to me. And I would be inclined to use at least as much if not more restraint than almost anybody in the authorization of such electronic eavesdropping devices.

Senator KENNEDY. You said earlier that the May Day type of demonstration wouldn't have presented to you a sufficient justification for finding that there was a clear and present danger. Wouldn't it be reasonable to assume, then, that there weren't any activities or individual——

Mr. KLEINDIENST. No, I didn't think 3,000 or 4,000 vandals could overthrow the Government of the United States. I thought that they might come in here and clog up the streets and burn automobiles and throw trash and boulders and try to block a bridge. And I felt that—we all felt that this Government had a duty to function. But to think that a bunch of people so disposed could overthrow this Government I think would be a joke. The only thing that happened on May Day was, instead of 4,000 or 5,000, there were 25,000 of them. And they accomplished one thing, they clogged up the jails and clogged up the courts, and made it impossible for policemen to use field arrest forms. But I think that is about all they did.

Senator KENNEDY. But do I gather——

Mr. KLEINDIENST. No, I wouldn't want to use electronic surveillance in that kind of situation.

Senator KENNEDY. How about individuals who were organizing for May Day?

Mr. KLEINDIENST. No.

Senator KENNEDY. That type of activity would not appear——

Mr. KLEINDIENST. Unless I got some information that some of the individuals were going to assassinate the President or going to kidnap public officials, or were going to blow up the Capitol—then I would say, they are starting now to threaten the institution of our Government, and this Government has a duty, by way of intelligence, to inform itself of that kind of conduct and to prevent it. But based upon the information that we have as to this bunch of people who came in on this, no.

Senator KENNEDY. So it has to be of that dimension, or that significance, in terms of those categories?

Mr. KLEINDIENST. Yes.

Senator KENNEDY. You said last June, I believe, on the Liz Drew show that "there should be some limits," on the warrantless taps, but you seemed to look only to the Supreme Court, which, you said, "over a period of time will carve and has carved out carefully what those limits are."

Could you tell us a little bit about what limits you believe have already been carved out by the Supreme Court?

Mr. KLEINDIENST. Well, subject of course to what the Supreme Court says—and that case is going to be argued tomorrow—I think they should be restricted to the national security. And then I think that the executive branch, in the fashion that President Nixon and Attorney General Mitchell have demonstrated, should see to it that only one person in the Government has the responsibility to authorize that, so that at all times there will be political responsibility for this kind of conduct. And I think that so long as there is that political responsibility, and so long as it is restricted to the national security, and so long as we have our Constitution and the President, who is charged with the preservation of it, I think, in my own opinion, they ought to have that power.

Senator KENNEDY. You don't see any kind of limitations that it would be appropriate for the Department of Justice to establish? Or do you want to just leave this completely up to the Supreme Court?

Mr. KLEINDIENST. The limitation, if I become the Attorney General, would be self-imposed restraint, Senator Kennedy. And I will be answerable to the Congress of the United States at any time with respect to that restraint.

Senator KENNEDY. And it would be guided by what you referred to earlier in terms——

Mr. KLEINDIENST. I am going to make the decision if I am the Attorney General, nobody else is, and it doesn't serve any useful purpose for me to publish a guideline which I could follow or not follow. A guideline is a commitment.

Senator KENNEDY. You said in Boston in May of 1970 that "each application for a warrantless tap—must be presented to the Attorney General personally with full supporting documentation."

Mr. KLEINDIENST. That is correct.

Senator KENNEDY. Could you describe for us just generally what this documentation would be, and what kind of factual situation would be necessary to support it?

Mr. KLEINDIENST. No, I can't, because I have never participated in any of those decisions, nor have I ever examined that. I think that is about the only

area in the Department of Justice in 3 years that I have not been involved in, and which Mr. Mitchell has not discussed with me, or which has not been delegated to me.

Senator KENNEDY. Does it bother you at all that you will be given this kind of responsibility but that there are no guidelines for you to follow? This is obviously an extraordinary kind of responsibility.

Mr. KLEINDIENST. Yes, it is.

Senator KENNEDY. And power and authority. I would think that you would either want or welcome at least some kind of guidance. Does it bother you that you don't have any?

Let's look at it from the other point of view—that one person has all this responsibility and authority, and it appears that there is very little, other than that person's own good judgment, that is used to limit or review that authority.

Mr. KLEINDIENST. Many of the awesome responsibilities of the Department of Justice bother me. But they are responsibilities that I am willing to assume. I would rather have them assumed by one person in a sensitive area like this than delegated to a committee and have happen what happened in the past frequently, where it was done but nobody would quite own up to it. And there was also an argument as to who did it, and why and when. And I think that is very bad. Yes, it bothers me, but I am willing to assume that burden.

Senator KENNEDY. What I was talking about was whether there shouldn't be some elaboration or some definition. Obviously it would be subject again to an interpretation of the words. But I would think that everyone, both the Congress and the American people, would feel better if they knew that there was just some paragraph some place, or just a page, that lays out the basis for it. I would think that you yourself would feel better about insuring that you are meeting your responsibility and even insuring that you are moving fast enough or far enough.

Mr. KLEINDIENST. That is something I would consider. But it would be as if I were writing myself a guideline. I wouldn't be adverse to considering it, Senator Kennedy. But I don't know if I will do it or not.

ANNUAL ELECTRONIC SURVEILLANCE REPORT AND WIRETAP INVESTIGATION

(Floor Statement by Senator John McClellan, May 10, 1971)

Mr. MCCLELLAN. Mr. President, on June 19, 1968, at 7:14 p.m. President Johnson signed Public Law 90–351, the "Omnibus Crime Control Act of 1968." Title III of the 1968 act, which I sponsored and which dealt with wiretapping and electronic surveillance, represented the culmination of an attempt, over the past 40 years, embracing approximately 50 bills, resolutions and joint resolutions, to arm law enforcement with a sorely needed tool to combat the forces of organized crime. District Attorney Frank S. Hogan, who has been one of the Nation's outstanding district attorneys for over 27 years, has aptly discribed this tool as: "the single most valuable weapon in law enforcement's fight against organized crime."

Title III of Public Law 90–351 has now been in effect for a period of 3 years. At first, it was not used on the Federal level, since it was the opinion of the then Attorney General that electronic surveillance was "neither effective nor highly productive," New York Times, May 19, 1967, p. 23, col. 1. Since January of 1969, however, title III has been used on the Federal level, and from January of 1969 through March of 1971, 315 court approved surveillance orders, including extensions, have been executed. All but 12 produced incriminating evidence. As a result, over 900 persons have been arrested, and, so far, 100 of these individuals have been convicted. Additional convictions will undoubtedly result as other defendants among those arrested are brought to trial. No case has yet reached the Supreme Court, but I am encouraged that the lower Federal courts have twice sustained the constitutionality of the basic scheme of the act. District Attorney Hogan's characterization of electronic surveillance on the local level is fast proving true on the Federal level, and the wisdom of the Senate in rejecting a motion to strike title III from the 1968 act by a record vote of 68 to 12 is being vindicated in practice.

Mr. President, when title III was enacted in 1968, seven States, including Arizona, Georgia, Maryland, Massachusetts, Nevada, New York, and Oregon, had State level legislation which dealt with wiretapping or electronic surveillance and authorized, under varying standards, the issuance of court orders for surveillance in criminal investigations. My research indicates that 19 States, including Colorado, Florida, Kansas, Minnesota, Nebraska, New Hampshire, New Jersey, Ohio, Rhode Island, South Dakota, Washington, and Wisconsin, now have such legislation and that the majority of it was patterned after title III. At least one of these post-title III statutes, moreover, has been sustained in a published opinion against constitutional attack in the State courts. *State* v. *Christy*, 112 N.J. Super. 48, 270 A 2d 306 (1970)). These developments, too, are heartening. If we can on the Federal and State level arm our police with the tools they so sorely need, I am hopeful that we can arrest and reverse the growth of organized crime in the United States.

Mr. President, under title 18, United States Code, section 2519, prosecutors who seek and judges who issue surveillance orders under the 1968 act or its counterparts on the State level are required to file detailed statistical reports in January of each year with the Administrative Office of the U.S. Courts and in April of each year, the Director of the Administrative Office is required to transmit to the Congress a summary and analysis of the data contained in these reports. These public disclosure provisions reflect the judgment of the Congress in 1968 that public accounting is essential to any system of the limited use of electronic surveillance techniques. Public support for the exercise of the power to wiretap and bug—even under court order—can only be obtained where the public is responsibly informed of the extent and character of its use.

Mr. President, the 1970 annual report has just been released by the Director of the Administrative Office. Because of the widespread interest in these matters of late, I think it will be helpful to summarize for the Senate and comment on the basic data in the report.

This is the third report submitted under title III. It covers the period from January 1, 1970, to December 31, 1970. It indicates that during this period 597 applications for orders were made to Federal and State judges. Of these applications, 183 were signed by Federal judges, and 414 were signed by State judges. Of the 414 State orders, 125 or 52 percent were issued in New York, while 132 or 32 percent were issued in New Jersey.

The 597 applications filed during the 12 months of 1970 compare with the 304 applications filed in 1969 and 174 filed in last 6 months of 1968. On the Federal level, the increase from 33 in 1969 to 183 in 1970 reflects the growth in the Department of Justice's drive against organized crime. Federal organized crime strike forces are now in operation in cities throughout the Nation. On the State level, the increase from 269 in 1969 to 414 in 1970, reflects the implementation of new laws in several States, primarily in New Jersey. In 1969, only 45 applications were made in New Jersey; in 1970, the figure rose to 132, of which the State attorney General's Office accounted for 82 in its increased organized crime efforts.

On the Federal level, of 183 authorized intercepts, 180 were installed and 43 extensions were granted. The 183 authorizations were granted for an average length of 17 days; the extensions for an average of 9 days. The State picture varied. In New Jersey, for example, of the 82 authorized intercepts of the attorney general's office, 82 were installed and 19 extensions were granted. The 82 authorizations were granted for an average length of 16 days; the extensions for 19 days.

In 1970, of the 583 applications that resulted in an intercept, 539 involved a telephone wiretap, 21 intercepts, used a nonconsensual listening device, such as a microphone. In 23 requests, both a telephone wiretap and a microphone were used for the interception.

The report does not, of course, include data on either the so-called national security or domestic security use of wiretaps or listening devices. In the national security area the use of these techniques, I should like to emphasize, was first begun as a result of a May 21, 1940, memorandum of President Franklin D. Roosevelt to Attorney General Robert Jackson, later Mr. Justice Jackson. In the domestic security area, this practice was first begun as a result of a July 17, 1947 memorandum of President Harry S. Truman to Attorney General Tom Clark, later Mr. Justice Clark. In both areas, it has been

continued in each administration and by each Attorney General thereafter. No reports in either of these two areas are required under the 1968 act, however, since the Congress in the 1968 act did not wish to limit in any fashion the constitutional power of the President as Commander in Chief of the Nation's Armed Forces to respond to either foreign powers or clear and present domestic threats to the survival of the Nation. See 18 U.S.C. 2511(3); 14 CONGRESSIONAL RECORD S6245–46—daily edition May 23, 1968. Nevertheless, the President recently commented on the number of wiretaps, indicating that none are currently in operation, while the number running at any one time in recent years has not exceeded 50. In the early 1960's, the figure was 100. What the scope of the President's constitutional power is in this area is a question the Congress did not reach in 1968, and which is, I note, now in the lower Federal courts winding its way up to the Supreme Court. See *United States* v. *Keith*, No. 71–1105 U.S. Court of Appeals for the Sixth Circuit, decided April 8, 1971.

The offenses specified in the applications summarized in the 1970 report covered a wide range of criminal activities. Several broad categories of crime, however, predominated: Arson 13; bribery, 16; drugs, 127; extortion, 17; gambling, 326; homicide, 20; larceny, 31; and robbery, 13.

The locations of the interceptions authorized included 203 residences, 163 apartments, 39 multiple dwelling, 122 business locations, and 30 business and living quarters.

The character of the interceptions were also described in the reports. In 1969, the average intercept involved 116 persons and 641 intercepts, of which 252 or 39 percent were incriminating. In 1970, on the other hand, the average intercept involved 44 people and 655 intercepts, of which 295 or 45 percent were incriminating. With more experience, therefore, it seems apparent that the intercepts are becoming more discriminating, a development that works well both for privacy and justice.

In certain areas, however, the picture is even better. In 1970, for example, on the Federal level, the average intercept touched on 57 persons and embraced 821 intercepts, of which 571 or 69 percent were incriminating, while in New Jersey, in the interceptions conducted by the office of the attorney general, 42 persons were involved and 294 intercepts were made, of which 237 or 80 percent were incriminating.

The total costs of each intercept—manpower and equipment—ranged from a low of $14 to a high of $146,300, with the average national intercept running $5,524, and the average Federal intercept running $12,106. These figures alone should do a great deal to put into context people's fear of excessive use of these techniques. Most police agencies including the Federal, simply do not have the manpower and other resources to conduct widespread surveillance.

Most of the cases in which there were interceptions reported are, of course, still under investigation or are awaiting trial. Nevertheless, the reports indicate that a total of 1,874 arrests have been made as of December 31, 1970. This figure compares favorably with the 625 arrested in 1969. Supplementary court action reports dealing with intercepts first reported in 1969 were also filed for 53 percent of the 1969 intercepts. Others are coming in periodically. A total of 31 trials and 70 convictions have occurred. One motion to suppress has been granted, one withdrawn, 25 are pending, and 25 have been denied. These figures, too, say a great deal about the judgment of those who say that these techniques are not effective or that they will be subject to widespread abuse. As the experience is beginning to develop, it shows clearly how important convictions can be obtained without an undue invasion of privacy.

Mr. President, I recognize, of course, that it is not proper to draw too many conclusions from wholly statistical information. Nevertheless, I am moved to point out and to emphasize that this data does not support the position of those who fought the enactment of title III and would now seek its repeal or substantial modification. The opponents of this legislation predicted widespread and promiscuous use of wiretaps and bugs by law enforcement authorities. They are being proven wrong. They said it was neither effective nor highly productive. Now they are being made to eat their words. I would hope, too, that when they make new and equally sweeping predictions and charges today that the Senate and the Nation will remember that their track record does not warrant paying close attention to them.

On the other hand, Mr. President, I am frank to admit that I sense a certain public concern about wiretapping. I have seen no evidence that warrants

it. I assure the Senate, too, that I have made it my business to watch carefully the implementation of this statute on the Federal and State levels. When and if abuses occur, I shall do all in my power to see to it that those responsible are prosecuted to the full extent of the law and shall seek from time to time to have appropriate inquiries made to verify that abuses are or are not taking place and to bring to the public's attention how well or ill these techniques for the investigation of crime serve the public interest.

It is in this context, therefore, that I should like to inform the Senate that I have directed the staff of the Subcommittee on Criminal Laws and Procedures, which I am privileged to chair and which has legislative oversight in the area of wiretapping and electronic surveillance, to begin to undertake a comprehensive examination of law and practice on the Federal and State levels. The Attorney General has informed me that he will extend to the subcommittee every possible assistance, and I am hopeful that this examination could mature into public hearings by early fall. There is a need here for a public review of the facts—all of the facts. Hopefully, these hearings can bring out those facts. I intend to do what is in my power to see to it that they do.

Mr. President, I ask unanimous consent to have printed in the RECORD following my remarks an exchange of correspondence between the Attorney General and myself, copies of the three Presidential memorandums, a staff memo summarizing the developments of the law in this area, certain summary charts contained in the 1970 Annual Surveillance Report, and excerpts from the President's recent news conference.

There being no objection, the items were ordered to be printed in the RECORD, as follows:

[Exhibit No. 1]

APRIL 28, 1971.

Hon. JOHN N. MITCHELL,
Attorney General of the United States,
Department of Justice,
Washington, D.C.

DEAR MR. ATTORNEY GENERAL: I write to solicit your cooperation in a study of wiretapping and electronic surveillance to be undertaken by the Subcommittee on Criminal Laws and Procedures.

As I am sure you are aware, I sponsored the enactment in 1968 of title III of Public Law 90–351, which deals with wiretapping and other forms of electronic surveillance, out of the deeply held desire both to strengthen law enforcement and to protect the legitimate need for privacy of our Nation's citizens. Title II of Public Law 90–351 will have been effective for a period of three years on June 19 of this year, a period during which it has been utilized on the federal level for 2½ years and in which the legislatures of 12 of our states have enacted comparable local legislation. I note, too, that the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, established by title III and recently strengthened by Public Law 91–644, will come into operation in June of 1973 to review the operation of title III and report to the President and the Congress two years thereafter. It is appropriate, therefore, now that we are at approximately the halfway mark of the initial six-year life of title III, that we take stock of where we are and chart carefully where it is that we might go.

As you may also be aware, after the first annual surveillance report had been issued in April of 1969 by the Administrative Order of the Courts, I directed the staff of the Subcommittee on Criminal Laws and Procedures, the Judiciary Subcommittee which has legislative oversight jurisdiction over title III, to undertake a review of the operation of the statute on the state level during its first six months of operation. The results of that study were presented to the Senate on August 11, 1969. (115 Cong. Rec. S 9569 daily ed., Aug. 11, 1969.) The study had immediate and beneficial effects, including a revision of the initial regulations issued by the Administrative Office for the annual reports so that they might more accurately reflect practices under the statute and the enactment of an amendment to title II itself as a part of Public Law 91–358, to clarify the civil liability of phone company and other private personnel cooperating in the execution of court orders issued under title III and fair on the face. I would hope that a similar study now could also have beneficial effects.

Since August of 1969, of course, a number of facets of the use of electronic

surveillance techniques have come into the focus of public attention, including their use in domestic security cases, a practice that I note was first established under President Truman and Attorney General Tom Clark in 1949, and the propriety and legality of recording and other techniques in light of the Supreme Court's decision in *United States* v. *White*, No. 13, October Term 1970, decided April 5, 1971.

In light of all these items, I believe, in short, that it would be in the public interest to undertake at this time a comprehensive review of law and practice in these and related areas. I would expect that this review could mature into public hearings by early fall. Should you agree that this course of action should be followed, please have an appropriate member of your staff contact the staff of the Subcommittee. I am sure that the details of the study can be worked out without undue difficulty.

With kindest regards, I am,

Sincerely yours,

JOHN L. MCCLELLAN.

[Exhibit No. 2]

MAY 7, 1971.

HON. JOHN L. MCCLELLAN,
U.S. Senate,
Washington, D.C.

DEAR SENATOR MCCLELLAN: This is in response to your letter of April 28, 1971 concerning a study of wiretapping and electronic surveillance to be undertaken by the Subcommittee on Criminal Laws and Procedures.

We at the Department of Justice are well aware, Senator, of your key role in the enactment of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the landmark legislation dealing with wiretapping and electronic surveillance, and of your interest in improving our law enforcement effort while at the same time safeguarding individual liberties. Our experience under the statute in the last 27 months has proved the wisdom of the framers of it on both counts.

We agree also that this is an appropriate time for us to report to the Congress on our experience under Title III, and for the Subcommittee on Criminal Laws and Procedures to undertake a comprehensive review of law and practice in the area of wiretapping and electronic surveillance, as well as related areas. You may be assured, therefore, of our full cooperation in the endeavor. Members of my staff will be in touch with the staff of the Subcommittee as you requested.

Sincerely,

_____,
Attorney General.

[Exhibit No. 3]

WIRETAPS

[From the Sunday Star, May 2, 1971]

Q. Mr. President, regarding the use of wiretaps in domestic security matters——

NIXON. The kind that you don't have with subpoenas, in other words?

Q. Yes, court orders. The attorney general has stated the policy on that and he has been criticized by Congressman Emanuel Celler of New York, who said that this could lead to a police state. Would you comment on the threat of a police state in the use of this type of activity?

A. Well, I have great respect for Congressman Celler as a lawyer and, of course, as the dean—as you know, he is the dean of all the congressmen in the House, a very distinguished congressman.

However, in this respect I would only say, where was he in 1961? Where was he in 1962? Where was he in 1963?

Today, right today, at this moment, there are one-half as many taps as there were in 1961, '62 and '63, and 10 times as many news stories about them. Now, there wasn't a police state in 1961, '62 and '63, in my opinion, because even then there were less than 100 taps and there are less than 50 today, and there is none, now, at the present time.

All of this hysteria—and it is hysteria, and much of it, of course, is political demagogery to the effect that "the FBI is tapping my telephone" and the rest—simply doesn't serve the public purpose.

In my view, the taps, which are always approved by the attorney general, in a very limited area, dealing with those who would use violence or other means to overthrow the government, and limited, as they are at the present time, to less than 50 at any one time, I think they are justified, and I think that the 200 million people in this country do not need to be concerned that the FBI, which, with all the criticism of it, which has a fine record of being non-political, non-partisan, and which is recognized throughout the world as probably the best police force in the world, the people of this country should be thankful that we have an FBI that is so greatly restricted in this respect.

This is not a police state. I have been to police states. I know what they are. I think the best thing that could happen to some of the congressmen and senators and others who talk about police states is to take a trip—I mean a trip abroad, of course—and when they go abroad, try a few police states.

This isn't a police state and isn't going to become one.

I should also point this out: Where were some of the critics in 1968 when there was Army surveillance of the Democratic National Committee—at the convention, I mean? We have stopped that.

This administration is against any kind of repression, any kind of action that infringes on the right of privacy. However, we are for, and I will always be for, that kind of action necessary to protect this country from those who would imperil the peace that all people are entitled to enjoy.

EXHIBIT NO. 4

TABLE 7.—SUMMARY REPORT ON AUTHORIZED INTERCEPTS GRANTED PURSUANT TO TITLE 18, UNITED STATES CODE, SEC. 2518, 1968,[1] 1969, AND 1970

Reporting period	Total	Residence	Apartment	Multiple dwelling	Business	Business and living quarters	Not indicated and other
Type of facility:							
June 20 to Dec. 31, 1968	174	67	49	10	45	----------	3
Jan. 1 to Dec. 31, 1969	302	135	68	14	71	5	9
Jan. 1 to Dec. 31, 1970	597	203	163	39	122	30	30

Reporting period	Total		Number of extensions	Average length (in days)			
	Authorized	Installed		Original authorization	Extension	Actual use	
						Days	Hours
Intercepts authorized:							
June 20 to Dec. 31, 1968	174	147	128	20	20	(1)	(1)
Jan. 1 to Dec. 31, 1969	302	271	194	26	22	9,019	3½
Jan. 1 to Dec. 31, 1970	597	583	246	22	19	11,200½	11

Reporting period	Total	Arson	Drugs	Extortion	Gambling	Homicide	Larceny	Robbery	All other
Major offense specified in application:									
June 20 to Dec. 31, 1968	174	2	71	13	20	21	19	8	22
Jan. 1 to Dec. 31, 1969	302	1	88	10	102	19	10	24	49
Jan. 1 to Dec. 31, 1970	597	13	127	17	326	20	31	13	50

Reporting period	Intercepts		Persons involved	Incriminating Intercepts
	Total [2]	Installed	Intercepts	
Average number per authorized intercept:				
June 20 to Dec. 31, 1968	174	147	29	454	98
Jan. 1 to Dec. 31, 1969	302	271	116	641	252
Jan. 1 to Dec. 31, 1970	597	583	44	655	295

Reporting period	Total where cost reported	Average	Less than $1,000	$1,000 to $2,000	$2,000 to $5,000	$5,000 to $10,000	$10,000 and over
Cost per authorized intercept:							
June 20 to Dec. 31, 1968	120	$1,358	75	21	18	6	----------
Jan. 1 to Dec. 31, 1969	262	2,634	127	45	54	24	12
Jan. 1 to Dec. 31, 1970	570	5,524	178	88	139	88	77

[1] Not available.
[2] Authorized by judges.

[EXHIBIT NO. 5]

TABLE 1.—JURISDICTIONS WITH STATUTES AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE OR ORAL COMMUNICATIONS EFFECTIVE DURING THE PERIOD JAN. 1, 1970 TO DEC. 31, 1970

State	Statutory citation	Reported use of wiretap in 1970	State	Statutory citation	Reported use of wiretap in 1970
Federal	18:2510 to 2520	Yes.	Nevada	200.610 to 200.690	No.
Arizona	13:1051 to 13:1059	Yes.	New Hampshire	570–A:1 to 570–A:11	Yes.
Colorado	40–4–26 to 40–4–33	Yes.	New Jersey	2A:156A–1 to 2A:156A–26	Yes.
Florida	934.01 to 934.10	Yes.	New York	813–J to 813–M; 814 to 825	Yes.
Georgia	26–3001 to 26–3010	Yes.	Oregon	141.720 to 141.900	No.
Kansas	22–2513	No.	Rhode Island	12–5.1–1 to 12–5.1–16	No.
Maryland	35–92 to 35–99	Yes.	South Dakota	23–13A–1 to 23–13A–11	No.
Massachusetts	272–99	Yes.	Washington	9.73.030 to 9.73.080	No.
Minnesota	626A.01 to 626A.23	Yes.	Wisconsin	968.27 to 968.33	Yes.
Nebraska	86–701 to 86–707	No.			

[1] Excludes jurisdictions which enacted legislation in 1971.

[Exhibit No. 6]

APRIL 30, 1971.

Memorandum to Senator MCCLELLAN.

From: G. Robert Blakey, Chief Counsel, Subcommittee on Criminal Laws and Procedures.

Subject: Wiretapping controversy.

You asked for a background memorandum on the current wiretapping controversy.

DEFINITIONS OF KEY TERMS

1. *wiretapping:* interception of communication transmitted over wire from phone *without* consent of participant.

2. *bugging:* interception of communication transmitted orally *without* consent of participant.

3. *recording:* electronic recording of wire or oral communication *with* the consent of a participant.

4. *transmitting:* radio transmission of oral communication *with* the consent of a participant.

5. *electronic surveillance:* generic term loosely used to cover all of the above, but often confined to "wiretapping" or "bugging."

6. *national security:* generic term loosely used to refer to wiretapping or bugging aimed at either "foreign" or "domestic" threats to the national security.

a. *foreign security:* usually meant to cover "wiretapping" or "bugging" to obtain coverage of foreign diplomats, spies, and their American contacts; also directed at Communist party and Communist front activities in the United States; sometimes used to obtain coverage of those involved in foreign intrigue, e.g., gun running to Latin American countries, etc.: primarily useful to prevent damage (theft of documents, etc.), not "solve crimes."

b. *domestic security:* usually meant to cover "wiretapping" or "bugging" to obtain coverage of extremist groups in the United States, e.g., the Black Panthers, groups within the K.K.K., and La Cosa Nostra; sometimes used to determine the influence of extremist groups in other legitimate organizations (civil rights or peace); primarily useful to prevent damage (assaults, bombings, kidnapping, homicides, riots, etc.).

Note that the "foreign" and "domestic" security distinction is sharper in theory than in practice. Often it is difficult without "wiretapping" or "bugging" to determine the "foreign" or "domestic" character of the threat.

Note, too, that since the emphasis is on the prevention of harmful activity rather than the punishment of those who have already caused harm, police action in these areas tends to cover more people for longer periods of time under less precise standards than conventional criminal investigations.

Caveat: Newspaper reporters, in particular, but all of us sometimes use "wiretapping," "bugging" and "national security" to refer to some or all of these techniques or areas of activity without carefully discriminating between them. This fact alone leads to most of the controversy; people often are not talking about the same things, even though they are using the same words.

CHRONOLOGY OF SIGNIFICANT EVENTS

1. *Olmstead* v. *United States*, 277 U.S. 438 (1928), held: (1) that wiretapping without a warrant did not violate the Fourth Amendment's ban on unreasonable searches and seizures because without a trespass there was no "search" and without a tangible taking there was no "seizure;" (2) that wiretapping did not violate the Fifth Amendment's ban on compulsory self-incrimination because no compulsion was placed on the speaker to speak; and (3) that the product of wiretapping illegal under state law may be used in Federal courts, since the suppression sanction applied only to violations of constitutional rules.

2. Section 605 of the Federal Communications Act of 1934, 48 Stat. 1103 (1934), 47 U.S.C. § 605 (1968), prohibited the "interception" and "divulgence" or "use" of the contents of a wire communication. At passage of the Act, managers of the bill observed, "[I]t does not change existing law." 78 Cong. Rev. 1013 (1934).

3. *Nardone* v. *United States*, 302 U.S. 379 (1937) held that the "divulgence" of a wiretap made by a Federal officer in a Federal court violated Section 605 of the 1934 Act.

4. N.Y. Const., Art. I, § 12 (1938), authorized wiretaps.

5. President Franklin D. Roosevelt on May 21, 1940, instructed Attorney General Robert H. Jackson to use wiretapping and bugging against subversive activities against the government of the United States. (A copy of this memo is attached.)

6. Attorney General Robert H. Jackson informed Congress in March 1941 that Section 605 could only be violated by both "interception" and "divulgence" or *private* "use." Hearings before Subcommittee No. 1 of House Judiciary Committee on H.R. 2266 and H.R. 3099, 77th Cong., 1st Sess. 18 (1941).

7. N.Y. Code of Crime Proc. § 813a (1942) implemented state constitution to authorize court-ordered wiretaps.

8. *Goldman* v. *United States*, 316 U.S. 129 (1942) held that bugging without a warrant did not violate the Fourth Amendment's ban on unreasonable searches and seizures if there was no trespass.

9. President Harry S. Truman on July 17, 1947, concurred in the recommendation of Attorney General Tom C. Clark that the F.D.R. authorization of 1940 be extended to cases of domestic security or where human life was in jeopardy. (A copy of this memo is attached.)

10. *On Lee* v. *United States*, 343 U.S. 747 (1952) held that the use of a transmitter by police officers without a warrant to overhear conversations between an informant and a suspect did not violate the Fourth Amendment's

ban on unreasonable searches and seizures where the informant consented to its use.

11. *Irvine* v. *California*, 347 U.S. 128 (1954) held that bugging without a court order accomplished by a tresspass violated the Fourth Amendment's ban on unreasonable searches and seizures, but that since the suppression sanction did not operate in state courts, no evidentiary consequences attached to the violation.

12. *Benanti* v. *United States*, 355 U.S. 96 (1957) held that a wiretap under a court order under New York law violated Section 605 of the 1934 Act and its product could not be used in a Federal court.

13. *Rathbun* v. *United States*, 355 U.S. 107 (1957) held electronic recording of a wire communication with the consent of a participant was not an "interception" under Section 605 of the 1934 Act.

14. *English Privy Councillors Report on Wiretapping* (1957) concluded that wiretapping under the Home Secretary's authorization was effective in criminal investigations, necessary to protect the security of the State, carried with it no harmful social consequences, and should be permitted to continue.

15. N.Y. Code of Crim. Proc. § 813a extended to authorize court-ordered bugging in 1959.

16. *Lopez v. United States*, 373 U.S.C. 427 (1963) held that electronic recording of an oral communication with the consent of a participant was not a violation of the Fourth Amendment's ban on unreasonable searches and seizures.

17. *Massiah* v. *United States*, 377 U.S. 201 (1964) held that electronic recording of an oral communication with the consent of a participant after the indictment of the suspect violated the suspect's Sixth Amendment right to counsel.

18. President Lyndon B. Johnson on June 30, 1965, prohibited the use of wiretapping or bugging by Federal agencies except to collect intelligence affecting the national security and on the approval of the Attorney General, (A copy of this memo is attached).

19. *Osborn* v. *United States*, 385 U.S. 323 (1966) held that electronic recording of an oral communication with the consent of a participant and pursuant to a court order was not a violation of the Fourth Amendment's ban on unreasonable searches and seizures.

20. Prime Minister Harold Wilson in 1966 re-affirmed the conclusions of the 1957 Privy Councillors Report but indicated that the Report's recommendations would not be followed to the extent that they would permit the interception of the wire communications of members of Parliament. Rept. C&P Pro. pp. 634–42 (17 Nov. 1966).

21. The President's Commission on Law Enforcement and the Administration of Justice in 1967 recommended that a carefully drawn statute be enacted to authorize court ordered wiretapping and bugging.

22. *Berger* v. *New York*, 388 U.S. 41 (1967) held that Section 813a of N.Y. Code of Crim. Proc. authorized unreasonable searches and seizures contrary to the Fourth Amendment, but the Court observed that where there was provision for judicial supervision based on an adequate showing of probable cause, particularization of the offense under investigation and the type of conversations to be overheard, limitations on the time period of the surveillance, a requirement of termination once the stated objective was achieved, close supervision of the right to renew and a return to be filed with the court, such surveillance could be reasonable.

23. Attorney General Ramsey Clark, on June 16, 1967, issued regulations that prohibited wiretapping and bugging except in national security matters and required that his approval be obtained prior to recording with or without a court order or transmitting.

24. *Katz* v. *United States*, 389 U.S. 347 (1967) held that bugging without a warrant violated the Fourth Amendment's ban on unreasonable searches and seizures, even though there was no trespass, where the communication was uttered under a reasonable expectation of privacy; *Olmstead* and *Goldman* were overruled, and the Court repeated that a carefully drawn court order would be sustained and expressly left open the question of national security wiretaps or bugging without a warrant.

25. Title III of Public Law 90–351 (June 19, 1968) provided as follows:

(1) prohibited all private wiretapping and bugging (18 U.S.C. § 2511(1)),

(2) permitted private recording only where not done to commit a tort or crime (18 U.S.C. § 2511(2)(d)),

(3) prohibited state or federal law enforcement wiretapping and bugging except under court order system (18 U.S.C. § 2511),

(4) permitted state or federal law enforcement recording (18 U.S.C. § 2511(2)(c)),

(5) expressly disclaimed any intent to regulate federal, foreign, or domestic security wiretapping or bugging (18 U.S.C. § 2511(3)),

(6) set up a Federal court order system for wiretapping or bugging (18 U.S.C. §§ 2516(1), 2518),

(7) set standards for optional state court order systems for wiretapping or bugging (18 U.S.C. §§ 2516(2), 2518),

(8) made unauthorized wiretapping or bugging a Federal civil tort (18 U.S.C. § 2529),

(9) required annual reports for Federal and state wiretapping and bugging (18 U.S.C. § 2519),

(10) set up a commission to review the operation of the first seven years of the statute in its seventh year (82 Stat. 223). (Note: P.L. 91–644 advanced this date from 1974 to 1973).

NOTE.—As of October 1970, the following 19 states had legislation for court ordered wiretapping or bugging:

Arizona (Post-*Berger*, Pre-Title III);
Colorado;
Florida;
Kansas;
Georgia (Post-*Berger*, Pre-Title III);
Maryland (Pre-*Berger*);
Massachusetts (Revised after *Berger* and Title III);
Minnesota;
Nebraska;
Nevada (Pre-*Berger*);
New Hampshire;
New Jersey;
New York (Revised after *Berger* and Title III);
Onio;
Oregon (Pre-*Berger*);
Rhode Island;
South Dakota;
Washington; and
Wisconsin.

26. The first Annual Surveillance Report for 1968 was issued; it indicated that 174 applications had been made and orders issued for wiretaps or bugs, which resulted in 263 arrests.

27. *Alderman* v. *United States*, 394 U.S. 165 (1969) held that illegally obtained evidence must be disclosed to suspects without an in camera review so that an opportunity can be afforded them to suppress evidence against them at trial.

28. The second Annual Surveillance Report for 1969 was issued; it indicated that 304 applications had been made and 302 orders issued for wiretaps or bugs, which resulted in 625 arrests.

29. Title VIII of Public Law 91–452 (October 15, 1970) set aside the result of *Alderman* for wiretapping and bugging occurring prior to June 19, 1968, and set up an in camera disclosure procedure.

Note: 18 U.S.C. § 2518(8)(d) and (10(a) govern disclosure of wiretapping or bugging after June 19, 1968 and provides for an in camera disclosure procedure.

30. *United States* v. *Clay*, 430 F.2d 165 (5th Cir. 1970), held that wiretapping under the direction of the Attorney General without a warrant to obtain foreign security intelligence did not violate the Fourth Amendment's ban on unreasonable search and seizure. (*Cert.* has been denied as to this issue.)

31. The American Bar Association on February 8, 1971 approved electronic surveillance standards for recording, wiretapping and bugging under court order and the use of such techniques in the foreign security field.

32. *White* v. *United States*, No. 13, October Term 1970, decided April 5, 1971, 9 Crim. L. Reptr. 3036 (4–7–71), sustained against Fourth Amendment objections the use of a transmittor by police officers without a warrant to overhear conversations between an informant and a suspect where the suspect consented to its use.

33. *United States* v. *Keith*, No. 71–1105, United States Court of Appeals for the Sixth Circuit, decided April 8, 1971, held that an authorization of a wiretap in a domestic security matters by the Attorney General without judicial sanction violated the Fourth Amendment's ban on unreasonable searches and seizures.

[Appendix A]

CONFIDENTIAL MEMORANDUM FOR THE ATTORNEY GENERAL

THE WHITE HOUSE,
Washington, D.C., May 21, 1940.

I have agreed with the broad purpose of the Supreme Court decision relating to wiretapping in investigations. The Court is undoubtedly sound both in regard to the use of evidence secured over tapped wires in the prosecution of citizens in criminal cases; aid is also right in its opinion that under ordinary and normal circumstances wiretapping by Government agents should not be carried on for the excellent reason that it is almost bound to lead to abuse of civil rights.

However, I am convinced that the Supreme Court never intended any dictum in the particular case which it decided to apply to grave matters involving the defense of the nation.

It is, of course, well known that certain other nations have been engaged in the organization of propaganda of so-called "fifth columns" in other countries and in preparation for sabotage, as well as in actual sabotage.

It is too late to do anything about it after sabotage, assassinations and "fifth column" activities are completed.

You are, therefore, authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigation agents that they are at liberty to secure information by listening devices direct to the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies. You are requested furthermore to limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens.

(S) F.D.R.

OFFICE OF THE ATTORNEY GENERAL,
Washington, D.C., July 17, 1946.

The PRESIDENT,
The White House.

MY DEAR MR. PRESIDENT: Under date of May 21, 1940, President Franklin D. Roosevelt, in a memorandum addressed to Attorney General Jackson, stated:

"You are therefore authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigating agents that they are at liberty to secure information by listening devices directed to the conversation or other communications of persons suspected of subversive activities against the Government of the United Sates, including suspected spies."

This directive was followed by Attorneys General Jackson and Biddle, and is being followed currently in this Department. I consider it appropriate, however, to bring the subject to your statement at this time.

It seems to me that in the present troubled period in international affairs accompanied as it is by an increase in subversive activity here at home, it is as necessary as it was in 1940 to take the investigative measures referred to in President Roosevelt's memorandum. At the same time, the country is threatened by a very substantial increase in crime. While I am reluctant to suggest any use whatever of these special investigative measures in domestic cases, it seems to me imperative to use them in cases vitally affecting the domestic security, or where human life is in jeopardy.

As so modified, I believe the outstanding directive should be continued in force. If you concur in this policy, I should appreciate it if you would so indicate at the foot of this letter.

In my opinion, the measures proposed are within the authority of law, and I have in the files of the Department materials indicating to me that my two most recent predecessors as Attorney General would concur in this view.

Respectfully yours,

(S) TOM C. CLARK,
Attorney General.

July 17, 1947.
I concur.

(S) HARRY S. TRUMAN.

THE WHITE HOUSE,
Washington, D.C., June 30, 1965.

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

I am strongly opposed to the interception of telephone conversations as a general investigative technique. I recognize that mechanical and electronic devices may sometimes be essential in protecting our national security. Nevertheless, it is clear that indiscriminate use of these investigative devices to overhear telephone conversations, without the knowledge or consent of any of the persons involved, could result in serious abuses and invasions of privacy. In my view, the invasion of privacy of communications is a highly offensive practice which should be engaged in only where the national security is at stake. To avoid any misunderstanding on this subject in the Federal Government, I am establishing the following basic guidelines to be followed by all government agencies:

(1) No federal personnel is to intercept telephone conversations within the United States by any mechanical or electronic device, without the consent of one of the parties involved. (except in connection with investigations related to the national security).

(2) No interception shall be undertaken or continued without first obtaining the approval of the Attorney General.

(3) All federal agencies shall immediately conform their practices and procedures to the provisions of this order.

Utilization of mechanical or electronic devices to overhear non-telephone conversations is an even more difficult problem, which raises substantial and unresolved questions of Constitutional interpretation. I desire that each agency conducting such investigations consult with the Attorney General to ascertain whether the agency's practices are fully in accord with the law and with a decent regard for the rights of others.

Every agency head shall submit to the Attorney General within 30 days a complete inventory of all mechanical and electronic equipment and devices used for or capable of intercepting telephone conversations. In addition, such reports shall contain a list of any interceptions currently authorized and the reasons for them.

(S) LYNDON B. JOHNSON.

REMARKS OF ATTORNEY GENERAL JOHN N. MITCHELL, BEFORE THE KENTUCKY STATE BAR ASSOCIATION, CINCINNATI, OHIO

Tonight I want to discuss two fundamental American rights: The individual's right of privacy and the people's right to preserve their form of Government.

Americans cherish their right of privacy, and they react strongly when they think it is threatened. At the outset, therefore, I want to speak candidly about recent efforts to frighten Americans into the conviction that their privacy is in jeopardy from an agency of their own Government. Specifically I refer to charges by a certain Senator and a certain Congressman against the Federal Bureau of Investigation and J. Edgar Hoover.

Let me set the record straight here and now.

Charge No. One: On April 14 the Senator made a lengthy speech claiming that the FBI makes "general political surveillance" of members of the Senate. He based this startling conclusion on the fact that FBI representatives had attended an Earth Day Rally last year where the Senator had been one of the speakers.

The FBI does not conduct general political surveillance of Senators, Congressmen or any one else. The reason the FBI attended the rally had nothing to do with the Senator. They were there only to observe certain persons whose known records indicated the possibility of violent or unlawful conduct. Indeed, one such person—who shared the speakers' platform with the Senator—was out on bail at the time under Federal conviction for inciting to riot. Let me ask you: If the FBI trailed a suspect to a ball game of the Cincinnati Reds, would Johnnie Bench have reason to think he was under surveillance?

The plain fact is that the Senator was not under surveillance and he knew he was not under surveillance. Yet he twisted the facts to make a political headline, and he owes an apology and a retraction to the FBI and Mr. Hoover.

Charge No. Two: On April 5 the Congressman stated flatly and unequivocally that the FBI "taps telephones of members of this body and members of the Senate"—and he later said he had "proof positive" to support his charges.

He even had the audacity to compare the FBI to Hitler's Gestapo.

His unproven charges were widely circulated, and he was repeatedly challenged by his colleagues and others to produce proof. Day after day he refused to do so. Yesterday he finally took the floor of the House and made a lengthy speech. It was full of adjectives, but not one iota of proof of the reckless charges he had made. Instead, it turned out that he thought he heard interference on his phone at home and suspected it was being tapped. He had it checked by the telephone company, which reported to him that his phone had not been tapped. The Congressman stated that the phone company always denies a tap that has been made by the FBI, so he said this proved his point. When "no" means "yes," I am reminded of the type of hypochondriac who insists he is sick, regardless of the doctor's assurances. The Congressman has been afflicted by a new type of paranoia—called tapanoia—the belief that your telephone is being tapped.

I repeat what I said at the time: The FBI has not tapped the telephone of any member of the House or Senate—now or in the past. And the Congressman also owes a full retraction and apology to Mr. Hoover and the FBI.

I do not want to mislead you into thinking there have been no investigations of Congressmen. Where there is probable cause to believe a Federal crime has been committed, the FBI has a duty to obtain evidence. I am happy to add that with two or three possible exceptions, members of Congress agree that they are entitled to no special immunity from the normal process of law. On rare occasions over the years, a members of Congress has indeed been the subject of normal investigative procedures—but not wiretapping—when the evidence indicated that such procedures were appropriate and necessary.

But with regard to the charges of general surveillance and wiretapping of Congressmen, those who are trying so hard to discredit the FBI for their own political purposes can't come through with the facts. All they have come up with is confirmation that the FBI is carrying out its statutory duties in the manner that the American people would want them carried out.

New let us move from the realm of fantasy to the real world of fact. As you know, the whole question of electronic surveillance has been evolving in the courts for many years. In the *Katz* decision of 1967, the Supreme Court held for the first time that the Fourth Amendment protects private conversations as well as private premises from "unreasonable searches and seizures." It also held that a prior court order is necessary for electronic surveillance. But it left open the question of whether such a court order is necessary in a situation involving the national security.

Taking this cue, Congress enacted some careful wiretapping legislation in 1968. Wiretapping by private parties was outlawed, but Government wiretapping was authorized in cases of specified serious crimes. Such wiretapping is strictly regulated by the need to get a court order from a judge after showing probable cause for belief that a crime has been or would be committed. The detailed requirements of the law actually provide more protection of privacy rights than does the warrant procedure that has long been established for physical searches and seizures.

Thus I cannot conceive how court-authorized wiretapping as such can continue to be a public issue, any more than making a search or seizure with a warrant. The principle has been set forth by the Supreme Court and the procedures have been spelled out by Congress.

I might add that its use has proven extremely effective in getting evidence that would otherwise be impossible against organized criminals. From January 1969 to March 1971, 315 Federal court-authorized wiretaps—including 51 extensions—were executed. All but 12 produced incriminating evidence. As a result, over 900 persons were arrested and so far, 100 of them were convicted. Additional convictions will undoubtedly result as other defendants among those arrested are brought to trial.

Far from being a source of public fear, as some would have us believe, court-authorized wiretapping provides added protection to the public against organized crime. Used with careful legal limitations, as it has been under the 1968 law, it is a positive benefit to the community.

Let me turn now to the other type of wiretapping that was also covered in the 1968 Act. Congress specifically excepted from the court order requirement the President's need to obtain information to protect the nation against foreign attack or against, and I quote, "the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government." This was also in conformity with Justice Byron White's concurring opinion in the *Katz* case, in which he wrote:

"We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable."

The fact is that such wiretapping had been used at least since 1940, when President Franklin D. Roosevelt called attention to the danger of "Fifth Columns" and authorized the Attorney General to use "listening devices" against "persons suspected of subversive activities against the Government of the United States, including suspected spies." He added, "You are requested furthermore to limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens."

Let me point out that national security wiretapping without a court order has been used by every subsequent Administration. Congress agreed in its 1968 law, believing that such wiretapping was outside the traditional type of judicial decision involving probable cause for a warrant. National security wiretapping is an executive decision, requiring a variety of national considerations other than judicial ones.

Since this 1968 legislation, the wiretap issue has continued to unfold in the courts. A distinction has been manufactured between so-called "foreign national security wiretapping" and so called "domestic national security wiretapping." Two Federal district courts have ruled that the "domestic" variety is unconstitutional without a court order. Two other district courts have ruled that such wiretapping is constitutional with a court order. The Sixth Circuit Court of Appeals, sitting here in Cincinnati, has upheld the contention of one of the district courts that so-called "domestic national security wiretapping" requires a court order.

I have made these brief historical references to make it clear that national security wiretapping is not a sudden invention of this Administration. What is new is the contention that national security wiretapping should be separated into "foreign" and "domestic," and that the latter should require a court order.

This raises a number of questions, which I would like to discuss.

Q. Mr. President, regarding the use of wiretaps in domestic security matters——

Answer: As you know, a court order is required to execute a wiretap in the prosectuion of a criminal offense. In order to obtain such a court order, considerable evidence must already have been gained to show "probable cause." Time is not of the essence in gathering such prior evidence.

But in a case where the national security is threatened, prevention is the first consideration. We first need intelligence on the movements of suspected conspirators, not formal evidence on which to convict them. In order for a national security wiretap to do any good it should come near the beginning of the investigation. Yet at that time we may not have enough evidence to show probable cause for a court order to wiretap. In fact, if we had such evidence we could probably prevent the threat in question without needing a wiretap.

I hope I have said enough to show that the requirement for a court order is appropriately applied to orthodox criminal-type wiretaps, but it does not fit the situation when applied to the national security field. By the time enough evidence is obtained to show probable cause, it may well be too late.

Question: Does a national security wiretap without court order conflict with the individual's right of privacy, and must it give way before that right?

Answer: Privacy is a precious right, but it is never absolute to the exclusion of other rights. The Fourth Amendment, which protects privacy, does not prohibit all searches and seizures. It prohibits only unreasonable searches and seizures. This contrasts to the unqualified guarantees in the First, Fifth and Sixth amendments. In fact, the courts have even indicated that the right of free speech set forth so clearly in the First Amendment must be weighed against other individual rights in such areas as slander, libel, plagiarism, copyright, and the right of privacy itself.

On the other hand, what about another right—the right of the public to protect itself and to preserve the government it has created? This right is implicit in the Constitution's very existence, and in the political theory on which it is based. I refer to the social contract by which man voluntarily gives up a degree of jungle liberty to a government of his own making, which in turn protects his liberties against jungle attack by others.

Preserving such a government is most certainly a right of the people who constituted it. As Abraham Lincoln said in his First Inaugural Address, "It is safe to assert that no government proper ever had a provision in its organic law for its own termination." And as I would add, the United States Constitution does not end with the words, "This document will self-destruct."

My point is that the issue of privacy must be considered in this dual context; where these two rights appear to conflict, then we must do what we can to preserve both as fully as possible. But neither commands our total allegiance while the other is dismissed out of hand.

Question: Does the tapping of telephone lines constitute a reasonable exercise of the Government's right of self-preservation?

Answer: It is not only reasonable in this context, but the proper authorities would be derelict if they did not use it. Where there is reason to believe persons are planning a violent attack on the existing structure of the Government, that Government is justified in finding out about those plans. It would be little comfort, after the Government had been overthrown by force, to say, "Well, we didn't feel we should eavesdrop."

Question: What about something less than the threat of actual overthrow? The bombing of the Capitol building? The assassination of a President? If we could prevent such monstrous acts through wiretap knowledge, do we have the constitutional right? In such cases should the Government's right to defend itself against violent attack prevail over the individual's right of privacy?

Answer: It must prevail, unless we wish to allow our orderly representative government to be disrupted. Liberty no less than security is endangered when government is prevented from governing.

Question: Should we distinguish between "foreign" national security wiretapping and "domestic" national security wiretapping?

Answer: How do we distinguish "domestic" and "foreign" enemies of our governmental structure? If they are aliens who are working on their own and are not connected with the government of another country, is their threat foreign? If they are American citizens directed by a foreign power, is the threat domestic? And while we are trying to find out which is which, may we tap a wire, or do we have to wait and search the rubble to find out?

If the institutions of our government have been destroyed, does it help to be able to say, "they have been destroyed from within?"

If this case seems too remote, let us look again at an occurrence that has been all too real. I refer to Presidential assassination, which certainly would fall under the classification of "a clear and present danger to the structure or existence of the Government." Since the Civil War four Presidents—Lincoln, Garfield, McKinley, and Kennedy—have been assassinated. Unsuccessful attempts were made on the life of one President-elect, Franklin D. Roosevelt, and one President, Harry Truman. None of these six deeds was done at the direction of a foreign power; I believe those who would make a distinction between foreign and domestic subversion would classify them as "domestic." At least two of them—the cases of Lincoln and Truman—were conspiracies. The question is, if it would have been possible to uncover these conspiracies and prevent them through wiretapping, should the Government have done so?

I would answer this with another question: Are we to stand by and let the plot unfold, so we can say, "Yes, it was a true-blue American bullet?"

Ladies and gentlemen, national security is indivisible. You cannot separate foreign from domestic threats to the Government and say that we should meet one less decisively than the other. I don't see how we can separate the two, but if it were possible, I would say that experience has shown greater danger from the so-called domestic variety. Either we have a constitutional government that can defend itself against illegal attack, or in the last analysis we have anarchy. The issue was eloquently expressed by Abraham Lincoln in his special message to Congress after the Civil War had begun.

"And this issue," he said, "embraces more than the fate of these United States. It presents to the whole family of man the question whether a constitutional republic or democracy—a government of the people by the same people—can or cannot maintain its territorial integrity against its own domestic foes. . . . It forces us to ask: Is there in all republics this inherent and fatal weakness? Must a government, of necessity, be too strong for the liberties of its own people, or too weak to maintain its own existence?"

This crucial question has resounded for more than a century since Lincoln. Obviously, we are still grappling with it today. Just as obviously, the answer lies in pursuing a fine balance between individual liberty on the one hand and collective survival on the other. So far we have maintained this balance as we have developed a sound body of constitutional law. But if we even choose unbridled liberty over government itself, we will soon have neither.

"WIRETAPPING AND OUR NATIONAL SECURITY"—AN ADDRESS OF JOHN N. MITCHELL, ATTORNEY GENERAL, BEFORE THE VIRGINIA STATE BAR ASSOCIATION, Roanoke, Va.

You have all, I am sure, heard and read a great deal in the past few months about one of the most controversial legal issues of recent times—that of national security wiretapping without a warrant. Because it involves the right to privacy, which all Americans cherish highly, and which this Government is dedicated to protect, the subject is fraught with deep emotional overtones.

The controversy has raged, both in the courts and in the press, and will continue to do so until the Supreme Court speaks to the issue. I would like to explore this issue with you, in hopes of dispelling some of the misconceptions that have arisen.

At the outset, let us consider the stakes involved in the Government's use of electronic surveillance in national security cases. Our success in counteracting hostile intelligence forces and domestic revolutionary elements depends on our ability to learn what they are doing. A key factor in accomplishing this has been the selective use of wiretapping.

The value of wiretapping in combatting foreign-directed espionage and subversion is widely recognized; it has been an integral part of the counter intelligence program of every major country.

The threat to our society from so-called "domestic" subversion is as serious as any threat from abroad. Never in our history has this country been confronted with so many revolutionary elements determined to destroy by force the Government and the society it stands for. These "domestic" forces are idealogically and in many instances directly connected with foreign interests.

In a speech on electronic surveillance Lewis F. Powell, Jr.—one of the nation's most distinguished attorneys and a former president of the American Bar Association—had this to say:

> The distinction between external and internal threats to the security of our country is far less meaningful now that radical organizations openly advocate violence. Freedom can be as irrevocably lost from revolution as from foreign attack.

In recent times, this nation has witnessed ever-increasing numbers of acts of sabotage. In August 1970, a bomb exploded in Sterling Hall at the Madison campus of the University of Wisconsin, killing one individual and causing damages estimated at three million dollars. The wave of terrorist bombings reached a climax with the brazen bombing of the U.S. Capitol early this year. These are not isolated incidents. According to statistics of the National Bomb Data Center, in the ten-month period from July 1, 1970 to May 1, 1971, there

were 1,378 bombings in this country—the vast majority of which were related to sabotage of the Nation's military efforts. In these bombings, 106 people were injured and 14 people were killed.

The selective use of wiretapping has been a vital part of the United States Government's defense against subversion for the last three decades. It has led to identification of hostile intelligence officers and their contacts and agents in the United States, disclosure of potential or actual defectors among U.S. nationals, detailed information concerning the *modus operandi* and intelligence methods of hostile agents, and exposure of connections between "domestic" subversive groups and foreign interests.

The argument for national security wiretapping does not rest on necessity alone; it has a very firm legal basis. It is this legal basis that I would like to emphasize in my remarks today.

In this Nation, the Government is constituted by the people and charged with the responsibility, in the words of the Preamble to the Constitution: "to insure the domestic Tranquility, promote the general Welfare, and secure the Blessings of Liberty." Overthrow of this Government by force and violence would be utterly inconsistent with the peaceful means for change provided by the Framers, and would deny to each citizen these securities to which he is entitled.

The Constitution designates the President as the Chief Executive and obligates him to "preserve, protect, and defend the Constitution of the United States." When the President enters upon his office, Article II, Section 1 of the Constitution requires him to solemnly swear that he will fulfill this obligation. This oath obviously does not refer to the defense of a piece of paper, but to the defense of the actual operation of the Constitution in prescribing the guidelines of Government. Were the President to permit the overthrow of that Government by unconstitutional means, he would be violating his constitutional oath. Nor does the President's oath differentiate between foreign and domestic enemies, requiring him to protect the Constitution against one but not against the other.

The Constitution of the United States cannot possibly be construed as containing provisions inconsistent with its own survival. It is the charter for a viable governmental system—not a suicide pact. Thus, a Presidential decision as to the steps to take in averting a clear and present danger to the national security cannot and should not wait until actual attack, sabotage, or insurrection have occurred.

Accordingly, the President has an obligation to collect, in advance and on a continuing basis, whatever information is reasonable and necessary for present and future decisions in using the forces at his command. No less can be expected of him if he is faithfully and dutifully to exercise his constitutionally imposed responsibility to protect the national security.

Persons intent on using illegal means to change or alter our form of Government do so covertly, and information as to their activities often can be obtained only in a covert fashion. Wiretapping has proven to be an effective method for obtaining such information.

The wiretapping question has been evolving in the courts for many years, and has been presented in various forms. Generally, these cases can be reduced to two prototypes: (1) wiretapping to obtain evidence in the enforcement of penal statutes, and (2) wiretapping to provide necessary intelligence information on a continuing basis to assist the President in discharging his duty to assure and preserve the national security.

In its landmark decision in *Katz* v. *United States*, rendered in 1967, the Supreme Court held for the first time that a wiretap initiated for prosecutive purposes in a criminal case constituted a search and seizure within the meaning of the Fourth Amendment. The Fourth Amendment does not proscribe all searches and seizures, but only those which are found to be unreasonable. Consequently, if it meets this test of reasonableness, wiretapping is a permissible governmental tool.

The Department of Justice has recognized that, when prosecutive information in a criminal case is sought, electronic surveillance—like most searches and seizures—requires a prior judicial warrant. In the litigation currently evolving in the courts, the Government has taken the position that the reasonableness standard of the Fourth Amendment is a flexible one and does not require in all cases that a warrant be obtained. It is our position that

compelling considerations exist when the President, acting through the Attorney General, has determined that a particular surveillance is necessary to protect the national security and that under these circumstances the warrant requirement does not apply.

It should be recognized that the Supreme Court has repeatedly held that under exceptional circumstances searches are reasonable though no warrant has been obtained. We believe that national security surveillance is of an exceptional nature and falls within this limited category. Pertinent here is the Court's explicit recognition in another case that "in applying any reasonableness standard, including one of constitutional dimension, and argument that the public interest demands a particular rule must receive careful consideration." The Supreme Court has never passed on the question whether "national security" surveillance is reasonable when conducted without a warrant, but Justice White, concurring in *Katz*, has written:

> We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.

The Congress has recognized that national security cases involve such compelling considerations. In response to the *Katz* decision, Congress enacted detailed wiretapping legislation in the Omnibus Crime Control, and Safe Streets Act of 1968. In that legislation, the Congress specifically set forth the standards that govern the granting of warrants for electronic surveillance in criminal cases. The Congress, however, carefully avoided imposing the warrant requirement in national security cases by including a provision in the statute which explicitly recognizes the President's authority to conduct such surveillances.

It is our position, given the long-standing practice of the Executive and the Congressional recognition of the necessity for distinguishing between wiretapping in ordinary criminal cases and in national security cases, that warrantless national security surveillances are reasonable within the meaning of the Fourth Amendment.

We have not argued against the need to get authorization for such a wiretap. Instead, we maintain that in national security cases the authorization required by the Constitution is that of the President of the United States, acting through his Attorney General, rather than that of a local magistrate.

It is not claimed that the President is exempt from the provisions of the Fourth Amendment, or that his discretion is unbridled. For any abuses of the power, the President is answerable not only to the electorate from whom all his powers are ultimately derived, but his decisions may also be reviewed by the courts in appropriate *in camera* proceedings. We simply say that the President's authorization of electronic surveillance for gathering intelligence in national security cases meets the requirement of reasonableness in the Fourth Amendment.

There are sound reasons for confining the authority to order electronic surveillance in national security cases to the President rather than to a multitude of lower court judges. The nature of the sensitive information involved in national security cases is not susceptible to evaluation by persons untrained in national security matters or to wide dissemination to persons not authorized by law to receive such information. Only the President is in a position to evaluate adequately such information in the light of various intelligence data submitted by the independent agencies within the intelligence community. We submit that the President, by virtue of his office and sources of information, is in a far better position than any magistrate to determine the need to initiate surveillance where the national security is at stake.

But if the authority to issue a warrant in national security cases is to be vested in magistrates only, the United States is left essentially with two options:

(1) To make disclosure to any one or more of over 600 members of the Federal judiciary who in most instances cannot be expected to have the necessary background to analyze the significance of the information disclosed or the necessity for the intelligence sought, or

(2) To become the only nation in the world unable to engage effectively in a wide area of counter-intelligence activities necessary to the national security.

These alternatives do not adequately protect the interests of privacy or of the security of citizens of the United States. Neither alternative, we submit, is acceptable and the Constitution does not require that we accept them.

It has been argued that the President might abuse his power to authorize national security wiretapping. This is put forward to challenge the "reasonableness" of a Presidential authorization, under the Fourth Amendment, and to insist that such authorization be made by the judiciary. Yet the courts that have questioned the constitutionality of the Presidential authorization on this ground are showing a remarkable inconsistency, which I will explain.

In 1803 the U. S. Supreme Court asserted its power to declare an act of Congress unconstitutional in the case of *Marbury* v. *Madison*. Chief Justice John Marshall emphasized that a Federal judge is required by his oath of office to discharge his duties "agreeably to the Constitution and laws of the United States." How could he do this, Marshall asked, if the Constitution "is closed upon him, and cannot be inspected by him? If such be the real state of things, this is worse than solemn mockery. To prescribe, or to take this oath, becomes equally a crime."

In challenging the President's power to authorize national security wiretapping, the Sixth Circuit Court of Appeals reasserted the power of the courts to make such judgments of constitutionality, drawing heavily on the *Marbury* v. *Madison* opinion. Yet the very argument of the courts' obligations under oath made in *Marbury* v. *Madison* must apply as well to the President's obligations under *his* oath—the more so since his oath is prescribed in specific words in the Constitution, while the judiciary's oath is not. The President's oath obligates him to "preserve, protect, and defend" the Constitution and the U. S. Government. To deny the President the means of obtaining intelligence on which to base actions in defense of that Government would be to deny him powers essential to the discharge of his oath. If this is the real state of things, to borrow Marshall's words, "this is worse than solemn mockery. To prescribe, or to take this oath, becomes equally a crime."

Since electronic surveillance is an effective means of gathering intelligence in national security cases, and is used by all major countries for such purposes, the President would be derelict if he did not use it where necessary and appropriate in defense of the constitutional Government.

Thus to claim that the President might abuse this power is the same as claiming that there should be no office with such power—an obviously self-defeating proposition. It is the same as arguing that the courts might abuse the power of constitutional review that Chief Justice Marshall found implicit in *his* oath. Such an argument was effectively answered not only in Marshall's *Marbury* v. *Madison* opinion, but also a number of years earlier by Alexander Hamilton, who wrote that "if it prove anything, would prove that there ought to be no judges."

Are we, then, to trust the courts to fulfill their oath of office without abusing it, but not trust the President in fulfilling his oath? Clearly the hard questions of government must be decided by someone. To withhold such basic powers from the President on the ground that they might be abused is to argue, in a paraphrase of Hamilton's words, "that there ought to be no President."

Finally, the distinction to which I alluded earlier—that between wiretapping in criminal cases and wiretapping in national security situations—is not the one that some lower Federal courts have today chosen to draw. Rather, they attempt to justify a distinction between so-called "foreign" national security wiretapping and so-called "domestic" national security wiretapping.

The use of the terms "foreign" and "domestic intelligence" and "foreign" and "domestic organizations" has resulted in a great deal of confusion and has created a dichotomy, which cannot be supported in law or fact. There is no dividing line between hostile foreign forces seeking to undermine our internal security and hostile "domestic groups" seeking the overthrow of our Government by any means necessary. I don't see how we can separate the two, but if it were possible, I would say that history has shown greater danger from the domestic variety.

As a legal proposition, what difference is there between the threat posed to the security of the United States by those who act as agents of a foreign power and that posed by an allegedly "domestic" organization? The Constitution requires the President to swear that he will "preserve, protect, and defend the Constitution of the United States." It does *not* say that he will "preserve, pro-

tect, and defend" it only against foreign agents, and that he must permit all others to destroy it if they will. It makes no distinction in its charge of responsibility to the President, and he can make none in his sworn duty to carry out that charge. You cannot separate foreign from domestic threats to the Government and say that we should meet one less decisively than the other. Either we have a constitutional Government that can defend itself against illegal attack, or in the last analysis we have anarchy. I firmly believe that the Constitution does not contain the seeds of its own destruction. Rather, it provides an enlightened basis by which man can prove that he can maintain both his freedom and his Government.

REMARKS OF WILLIAM H. REHNQUIST, ASSISTANT ATTORNEY GENERAL, OFFICE OF LEGAL COUNSEL, AT A PANEL DISCUSSION ON PRIVACY AND THE LAW IN THE 1970'S, AT THE AMERICAN BAR ASSOCIATION CONVENTION, LONDON, ENGLAND

"LAW ENFORCEMENT AND PRIVACY"

Since accepting a position in the United States Department of Justice some two and a half years ago, I have found myself asked to speak on a variety of subjects on which my opinion as a private citizen would have been of interest to very few persons, indeed. Most of these subjects are ones about which I knew virtually nothing at the time I became an Assistant Attorney General; whether I am less ignorant two and a half years later you will be better able to judge at the close of my remarks than now. I have tried, though perhaps not always successfully, to avoid following the rather facetious advice that Arthur Balfour is said to have given Lord Halifax shortly after the latter was first elected to Parliament. Lord Halifax, in his memoirs, says that he consulted Balfour, then the leader of the Conservative Party, as to an appropriate subject and length for his maiden speech in the House of Commons. Balfour told him, said Halifax:

> "Speak as often and as long as you can on every occasion. You will rapidly develop that utter contempt for your audience which is the hallmark of every true bore."

The subject of "Privacy and the Law in the 1970s" is without doubt one of the fundamental social and political issues of this decade. Discussion, say nothing of solution, of the many problems which it poses cannot profitably be advanced by generalized praise of good or denunciation of evil. While today I am going to address myself, in keeping with the suggestion of the panel chairman, to the relationship between law enforcement and privacy, it is well to bear in mind that this is but one of the problem's facets. The "information explosion", as it has been termed by some commentators, has resulted in part from an almost geometrical increase in federal benefit programs in the United States in the last three or four decades. I suspect the experience in Great Britain has not been dissimilar. I think the distinction between what I would call administrative information gathering—the obtaining of information from citizens for the purpose of conducting a census, administering a governmental pension or health program, and other functions such as this—as opposed to the investigative intelligence gathering of the law enforcement arm of the government—deserves special emphasis, because the difference between these two functions produces essentially different considerations of privacy policy in the equation. My remarks today are addressed only to the gathering of criminal investigative intelligence.

The United States, of course, has a federal system of government, in which both the national law enforcement function and the state law enforcement functions are substantially independent of one another, subject only to the overriding commands of the Constitution. The President, as Chief Executive, is charged with the duty "to take care that the laws be faithfully executed", and it devolves upon the Department of Justice to enforce a wide variety of criminal statutes which have been made a part of the federal law by Congress. State governments discharge a similar function through offices of local prosecutors and through the office of the state attorney general.

I think analysis in terms of privacy is best served by distinguishing at least three different types of law enforcement activities which may be said to raise privacy problems.

First, there are the efforts on the part of what I shall refer to generically as the "government" to compel the production of evidence, either testimonial or documentary. This may occur as a result of an administrative subpoena, it may occur in a grand jury proceeding, or it may occur at the actual trial of the case. Traditionally this area has been thought to involve the traditional criminal law type safeguards—the privilege against self-incrimination, the right to counsel, the requirement of materiality, and the like. While it may have remote privacy implications, they have not figured prominently in the current privacy debate in the United States.

Second, there is the authority of the government to search persons, dwellings, automobiles, and other nonpublic areas for evidence which may lead to the solution of a crime. In the United States, such authority is limited by the Fourth Amendment to our Constitution, prohibiting unreasonable searches and seizures.

One area of this branch of governmental authority—wiretapping—has been a subject of considerable debate in our country, and I shall address it in more detail in a moment.

Third, there is the question of the extent to which the government may properly observe persons and activities conducted in public places—meeting halls, amphitheaters, streets, and parks. Some of those concerned with privacy have insisted that limitations, either legislative or constitutional, be placed on governmental activity in this area, while on the other hand those charged with responsibility for law enforcement have felt that many of the proposed limitations would seriously hamper the law enforcement function without producing a correspondent social benefit in the increased privacy that would be available to citizens. To this subject, also, I shall return in more detail in a moment.

Wiretapping

"Wiretapping" in its more limited sense refers to the interception of a telephonic communication of which the parties to the conversation are unaware. Loosely used, it can include "bugging"—the placing in a room, unbeknownst to its occupants, or on a party to a conversation, unbeknownst to the other parties, a transmitting device which will either record the conversation itself or transmit it to some other place where it will then be recorded. These latter manifestations are frequently associated with the use of undercover informants, who, though they are in the confidence of a suspected group of criminals, are nonetheless in the employ of the government.

There is something a little bit on the seamy side about all of these procedures, and in an ideal society their lack of social usefulness would doubtless cause them to be prohibited. Since the society in which we live—I speak for the United States, but I suspect the same is true here—is not ideal, the question is whether the admitted infringements on expected privacy which these methods of investigation give rise to are justifiable in terms of the aid they provide in the solution of serious and extensive crime.

In the United States, the Supreme Court about 45 years ago held that wiretapping was not a violation of the Constitution. Congress shortly afterward by statute prohibited the divulgence or use as evidence in the federal courts of information obtained through wiretapping. Less than five years ago, the Supreme Court overturned the earlier decision, and held that wiretapping was a form of "search and seizure" within the language of the Fourth Amendment to our Constitution. The Court indicated in that decision, and in other decisions rendered about that time, that a statutory authorization for wiretapping, providing for the rough equivalent of a warrant prior to the commencement of the tap, would be constitutional. Congress followed the Court's suggestion, and in the Omnibus Crime Act of 1968 authorized wiretapping under this sort of supervision.

There is no question that the vastly expanded use of electronic means of communication, and the vastly increased efficiency of the technology of interception and overhearing, have made wiretapping in its more general sense a more potent weapon for law enforcement personnel than it was forty or fifty years ago. But during this same forty or fifty years we in the United States have witnessed the burgeoning of what is loosely called "organized crime", which has attached its tentacles to more than one legitimate business or industry in our country. It, too, has increased apace with and through the use of modern technology.

The present Administration of the Department of Justice in the United States is committed to the use of wiretapping under the safeguards prescribed by Congress, and under the administrative safeguard requiring each application for a warrant to be personally authorized by the Attorney General. The commitment is based in large part on the fact that an effective attack on organized crime cannot be mounted without wiretapping.

When we deal with the activities of organized crime, we deal with the most sordid sort of trafficking in drugs, prostitution, and gambling, as well as in illegitimate aberrations of legitimate business. Persistent efforts, not always unsuccessful, to corrupt local law enforcement officials; murder, committed by anonymous hired guns, are its trademarks. Normal detection techniques in the tradition of Sherlock Holmes, Hercule Poirot, and the long succession of Scotland Yard inspectors who have been immortalized in print, are of far less use here. The faceless killer never knew the victim, and may never have seen him before; the bagman is an easily replaceable hood at the lowest level of the organization. The heads of these syndicates perform no criminal act themselves; they simply instruct others to perform them for him. Painstaking and imaginative sifting of readily available evidence, which may solve the murders envisioned by Arthur Conan Doyle and Agatha Christie will scarcely dent the upper echelons of organized crime.

Thus, the structure of crime in this area has changed just as dramatically as technology. If law enforcement methods do not somehow keep pace with these changes we must virtually write off the hope for making substantial inroads into this widespread and sinister form of criminal activity.

Is the invasion of privacy entailed by wiretapping too high a price to pay for a successful method of attacking this and similar types of crime? I think not, given the safeguards which attend its use in the United States. The Attorney General must report to Congress the total number of federal applications for wiretapping made each year, and the report he furnished indicated that last year the federal government sought 183 wiretap warrants. This is not a "pervasive" use of wiretapping, using that adjective in its narrowest possible sense. It is instead a restrained and careful use of that technique which has led to series of genuinely significant arrests and convictions in the field of organized crime in the past three years.

In the limited area of what are described for want of a better word as "national security" investigations—the executive branch in the United States for more than thirty years has asserted the right to wiretap without securing any Fourth Amendment type of warrant. This position has been taken through the Administrations of six successive Presidents of the United States, dating from Franklin D. Roosevelt, and it is the government's position that the practice is both consistent with the Fourth Amendment and necessary to the effective protection of the national security. The practice has recently been the subject of sharp and quite widespread criticism. The issue has been submitted to several federal district courts and one court of appeals, which have reached differing results. The Supreme Court has agreed to decide the issue in its next term, at which time the issue of the legality of the practice will be settled. Whatever may be the ultimate decision by our highest Court on the merits of the question, I believe that a refusal of the Justice Department, in its role as advocate before the courts for the executive branch of the government, to vigorously argue in favor of its legality would be a wholly unwarranted abdication of the Department's responsibility.

Surveillance

To what extent may law enforcement officials properly observe members of the citizenry in public places? It has been suggested by at least one prominent figure in the privacy debate in our country that no suspect ought to be subject to such surveillance unless there is "probable cause" to believe that he is guilty of committing a crime. The imposition of such a standard, in my view, would be a virtually fatal blow to law enforcement.

At the outset of an investigation, law enforcement officers are confronted with the fact that a crime has been committed, and with varying numbers of "leads" which may or may not offer some hope for its ultimate solution. Every such lead must be run down if a solution is to be effected, even though the great majority of leads turn out to be dead ends. Frequently, in the process of running down dead-end leads, investigative attention turns to

people who later prove to be entirely innocent of any offense. But their innocence can be known only in retrospect; the ultimately productive lead may look no better than the unproductive ones at the time an investigation has begun.

In view of the very nature of the investigative process, it would be highly unrealistic to require that there be "probable cause" to suspect an individual of having committed a crime in order that his activities may be inquired into in connection with the investigation of the crime. Quite the contrary, probable cause—for an arrest or specific search—is hopefully to be found at the conclusion of an investigation and ought not to be required as a justification for its commencement.

The basic limitation which may properly be placed on investigative authority is that it must be directed either to the solution or to the prevention of a crime, and that it pursue leads reasonably believed to aid in that activity.

In the United States we have recently had experience with the collection of what may be loosely called "civil-disturbance" information by Army intelligence sources, rather than by regular law enforcement officials. This program, begun about five years ago because of the same generally agreed need for a great deal more information about potential trouble spots in urban centers, tended to become broader and broader in scope as it filtered down the echelons of the Army command. Examples have recently been adduced of Army intelligence files kept on prominent public figures, and consisting largely of newspaper accounts of the statements made by these figures on current political issues. Whatever may have been the merits of the program in its inception, it rather clearly got out of hand. That program has been discontinued by the present Administration. The cataloging of the opinions of citizens, public or private, on the issues of the day is not a proper function of government in a free society. The collection of genuine civil disturbance information, to the limited extent necessary under federal law, has now been returned to the regular law enforcement branches of the government.

Who Shall Regulate the Regulators?

Many of those deeply concerned with privacy in our country feel that either by court decree or legislation the extent of law enforcement activities in the fields which I have discussed should be sharply curtailed. Implicit in their suggestion is that somehow the Executive Branch of the United States Government is not in any sense responsible to the public will and that controls must be imposed by any other branches on the Executive Branch. While our Executive is separate from the Legislative Branch, rather than directly responsible to it, it is surely ultimately responsible to the electorate of the Nation. The President stands for reelection every four years, and must at that time—as well as at frequent intervals in between—defend his stewardship of Executive power.

As to the merits of proposed legislative or judicial curtailment of the investigative authority of law enforcement agencies, I simply do not believe that a limitation on the investigative activities of law enforcement officials engaged in seeking the solution to crime would be either desirable or workable. If such a restriction were to have teeth in it, it would necessarily involve judicial review of an investigation, not at its end, but at its commencement. The opportunity for skillful defense lawyers to obtain information of great value to their clients, and to seriously delay a legitimate investigation, would be greatly enhanced by the availability of such a proceeding.

On the other hand restriction of the dissemination of information gathered in the process of criminal investigation is quite appropriate and desirable. Certainly the casual release of such information by law enforcement officials to persons outside the Government who have no legitimate need to have it is reprehensible. It is presently prohibited by regulation in the Department of Justice, and in many other law enforcement agencies. The embodiment of this sort of prohibition in a statute which was the result of a careful balancing of the competing interests would doubtless be entirely acceptable to those engaged in law enforcement.

I hope in my presentation this morning I have given you some idea about how the United States Department of Justice approaches the questions of surveillance and personal privacy, and the balance that must be struck between the two. It is quite possible to select from among countless government activities instances of clear abuse of the individual right of privacy, and to

draw from these relatively isolated examples the conclusion that we are reaching an age of social control similar to that depicted by George Orwell in his novel, *1984*. Neither in the United States nor, I suspect, in this country, is *1984* nor anything like it upon us. The legitimate concern over privacy is not advanced by those who mount an unselective attack on the government in terms of a highly fictitious "dossier dictatorship", or by those who speak in terms of the government's "pervasive" wiretapping. The statistics I cited earlier should put to rest such exaggerations. Intelligent discussion of this subject cannot but lead to the conclusion that neither government surveillance nor individual privacy can be treated as an absolute or paramount value at the expense of the other. We cannot allow our zeal for effective law enforcement to erode the rights essential to a free citizenry, but we must be equally certain that in our concern to preserve the right of privacy to the law abiding, we do not unwittingly assure anonymity for the criminal. One of the great virtues of the Anglo-Saxon legal tradition shared by Great Britain and the United States has been its ability by rational accommodation to preserve surprisingly large elements of each of two competing values. I do not doubt that it will prove capable of resolving the conflict of the seventies between law enforcement and privacy.

EXCERPTS FROM PRESS CONFERENCE OF JOHN N. MITCHELL, ATTORNEY GENERAL

Question. Mr. Attorney General, it's getting to the point where I wonder if the Justice Department can do something about the individual who thinks his line is tapped and doesn't known how to check this.

If the individual checks with the telephone company, he gets nowhere, and Senator Yarborough said the other day he felt sure his line was tapped and probably the lines of all the Senators.

Is there any place where an individual can go now in Government to have his rights protected and checked out?

Mr. MITCHELL. Certainly. He can go to the Justice Department. As far as Senator Yarborough's statement that you repeat, I am not aware of it. I can tell you flatly, from the Justice Department's standpoint, and all the other agencies in the Government that are obligated to comply with Justice Department regulations, that it would be inconceivable for even a consideration of placing a telephone tap on any Members of Congress or anybody else in Government.

With respect to the individual citizen, unless they are involved in organized crime or in the process, or have committed a crime, they have no concerns whatsoever. We have used the powers that we have with respect to wire tapping very, very sparingly, and we expect to continue to do so. So that any citizen in this United States who is not involved in some illegal activity has no concern whatsoever.

Question. How many taps are now in, Mr. Attorney General? And bugging?

Mr. MITCHELL. There are fewer taps and bugging presently on than when I came into office.

Question. Can you give us a number?

Mr. MITCHELL. No, sir, I cannot.

Question. Can you tell us how many you have approved?

Mr. MITCHELL. No, sir, I cannot.

Question. Can you tell us how many did you take off?

Mr. MITCHELL. Quite a number.

Question. Why did you take them off?

Mr. MITCHELL. After reexamination of the situation that existed, it was determined by various agencies involved in the Department of Justice that they were not productive.

Question. What about the latest edict that the Department has the right to tap the phone—to go into the telephones of anybody whom the Department considers dangerous to the security of the United States?

Mr. MITCHELL. Let me put it in this context: I presume you are referring to the papers that were filed in the Chicago case.

As you can well imagine, those electronic surveillances were placed on long before my coming into office. The purpose of those electronic surveillances was to protect the National security, both internal and foreign.

And it has been the position of this Department in that proceeding out there, which we will maintain so long as the Courts support us, that this is a power vested in the President of the United States to protect the foreign and internal security of this country, and we will try and sustain, and expect to sustain, the power of the President and this Government to act accordingly.

* * * * * * *

Question. Mr. Attorney General, your predecessor Ramsey Clark said that wire tapping was not productive. The Nixon Administration promised to make greater use of wire tapping. You say now you have reduced the number of wire taps.

Have you come around to Mr. Clark's way of thinking?

Mr. MITCHELL. Quite to the contrary. You see, this Administration has taken advantage of the provisions of the Safe Streets Act with respect to the use of wire tapping in the area of organized and other types of crime.

We have used it in that field and we find it very productive. In fact, the first wire tap that I used in connection with organized crime broke one of the largest narcotics cases we have had in this country in some time.

So it's a distinction between reducing its use in the foreign field, national security, and its implementation under the Safe Streets Act with respect to the crime area.

Question. When you say that you have reduced the number of taps, you are referring specifically to taps authorized by the Department of Justice regarding the foreign intelligence? That doesn't mean that overall wire tapping has been reduced?

Mr. MITCHELL. No, I said that the total number of taps had been reduced, including both areas.

* * * * * * *

Question. Are there currently any wire taps or bugging devices being used against any civil rights leaders in the country at this time?

Mr. MITCHELL. I don't know what you describe as civil rights leaders, but I would say in the normal connotation of the term, the answer would be no.

Question. Do you have any requests from the Director of the FBI to do so at this time?

Mr. MITCHELL. Do I have a request from him to bug the lines of civil rights leaders? No.

Question. There is an important distinction between tapping and bugging, and you made it once in your preliminary remarks, but not in some other references.

When you said there was no wire tapping of Congressmen and Government officials, did you also mean bugging and related electronic surveillance devices? And when you spoke of a reduction in the number of taps, does that also apply to other electronic surveillance devices?

Mr. MITCHELL. I used electron surveillance throughout, or intended to. Obviously there is—there is no electronic surveillance of any Congressman or people in Government, and of course there is no investigation of them, or anything else.

This would be completely foreign to the activities of this Department.

* * * * * * *

REMARKS BY PRESIDENT NIXON AT THE ANNUAL CONVENTION OF THE AMERICAN SOCIETY OF NEWSPAPER EDITORS, APRIL 16, 1971

SURVEILLANCE BY GOVERNMENT AGENCIES

Mr. RISHER. Mr. President, I would like to get back to Mr. Hoover and the FBI. Is there any credence to the complaints by some Congressmen, as far as you know, that they are under surveillance by the FBI?

The PRESIDENT. Well, Mr. Risher, let me answer that question in terms of what I know, because I checked this personally. I was in the House, I was in the Senate, and I am very jealous of the right of Senators and Congressmen, and every citizen actually, not to have surveillance when he is engaged in public activities. Particularly, I can assure you, that there is no question in

my mind that Mr. Hoover's statement that no telephone in the Capitol has ever been tapped by the FBI is correct. That is correct.

The case you referred to, the Dowdy case, did not involve the tapping of a Congressman's telephone.

The second point that I should make is this: Let's get this whole business of surveillance and the rest into some perspective. First, when we talk about police states, there are 205 million people in this country.

Did you know, even the Nation's editors, sophisticated as you are, that over the past 2 years there were only 300 taps by the FBI through court orders?

Do you know what was accomplished from those taps? There were 900 arrests and 100 convictions, and particularly convictions in the important area of narcotics where millions and millions of dollars worth of narcotics that otherwise would have gone to the young people of America were picked up? That was why those taps were carried on.

Now let's talk about the other area which I think Mr. Risher and the people are more concerned about. They say what about the taps that are not made by court order but that are made for the national security? I checked that, too. The high, insofar as those taps are concerned, were in the years 1961, 1962, and 1963. In those years, the number of taps was between 90 and 100. Now, in the 2 years that we have been in office—now get this number—the total number of taps for national security purposes *by the FBI*, and I know because I look not at the information but at the decisions that are made—the total number of taps is less, has been less, than 50 a year, a cut of 50 percent from what it was in 1961, '62, and '63. As far as Army surveillance is concerned, once we saw what had happened to the Democratic National Convention, that had even been carried to the surveillance of Adlai Stevenson, who later became a Senator, we stopped them.

I simply want to put this all in perspective by saying this: I believe the Nation's press has a responsibility to watch Government, to see that Big Brother isn't watching.

I don't want to see a police state. I argued the right of privacy case in the Supreme Court and I feel strongly about the right of privacy. But let's also remember that the President of the United States has a responsibility for the security of this country and a responsibility to protect the innocent from those who might engage in crime or who would be dangerous to the people of this country.

In carrying out that responsibility, I defend the FBI in this very limited exercise of tapping.

One final point: You talk about police state. Let me tell you what happens when you go to what is really a police state.

You can't talk in your bedroom. You can't talk in your sitting room. You don't talk on the telephone. You don't talk in the bathroom. As a matter of fact, you hear about going out and talking in the garden? Yes, I have walked many times through gardens in various places where I had to talk about something confidential, and you can't even talk in front of a shrub. That is the way it works.

What I am simply saying is this, my friends: There are police states. We don't want that to happen to America. But America is not a police state, and as long as I am in this office, we are going to be sure that not the FBI or any other organization engages in any activity except where the national interests or the protection of innocent people requires it, and then it will be as limited as it possibly can be. That is what we are going to do.

Mr. DICKINSON. Thank you very much, Mr. President, thank you.

NOTE:—The President spoke at 9 p.m. in the Regency Ballroom at the Shoreham Hotel. His remarks were broadcast on radio.

EXCERPT FROM PRESIDENT NIXON'S PRESS CONFERENCE, MAY 1, 1971

WIRETAPS

Q. Mr. President, regarding the use of wiretaps in domestic security matters——

The PRESIDENT. The kind that you don't have with subpoenas, in other words?

Q. Right, without court orders. The Attorney General has stated the policy

on that and he has been criticized by Congressman Emanuel Celler of New York, who says that this could lead to a police state. Would you comment on the threat of a police state in the use of this type of activity?

The PRESIDENT. Well, I have great respect for Congressman Celler as a lawyer and as, of course, the dean—as you know, he is the dean of all the Congressmen in the House, a very distinguished Congressman. However, in this respect I would only say, where was he in 1961? Where was he in 1962? Where was he in 1963?

Today, right today, at this moment, there are one-half as many taps as there were in 1961, '62, and '63, and 10 times as many news stories about them. Now, there wasn't a police state in 1961 and '62 and '63, in my opinion, because even then there were less than 100 taps and there are less than 50 today, and there is none, now, at the present time.

All of this hysteria—and it is hysteria, and much of it, of course, is political demagoguery to the effect that the FBI is tapping my telephone and the rest—simply doesn't serve the public purpose. In my view, the taps, which are always approved by the Attorney General, in a very limited area, dealing with those who would use violence or other means to overthrow the Government, and limited, as they are at the present time, to less than 50 at any one time, I think they are justified, and I think that the 200 million people in this country do not need to be concerned that the FBI, which has been, with all the criticism of it—which has a fine record of being nonpolitical, nonpartisan, and which is recognized throughout the world as probably the best police force in the world, the people of this country should be thankful that we have an FBI that is so greatly restricted in this respect.

This is not a police state. I have been to police states. I know what they are. I think that the best thing that could happen to some of the Congressmen and Senators and others who talk about police states is to take a trip—I mean a trip abroad, of course [*Laughter*]—and when they go abroad, try a few police states.

This isn't a police state and isn't going to become one.

I should also point this out: Where were some of the critics in 1968 when there was Army surveillance of the Democratic National Committee—at the convention, I mean? We have stopped that.

This administration is against any kind of repression, any kind of action that infringes on the right of privacy. However, we are for, and I will always be for, that kind of action that is necessary to protect this country from those who would imperil the peace that all people are entitled to enjoy.

STATEMENT OF DEPARTMENT OF JUSTICE

In response to erroneous and misleading allegations made by Senator Kennedy in a letter to other senators concerning electronic surveillance, the Department of Justice issued the following statement today:

In the interest of protecting the security of the United States, it is necessary to use electronic surveillance devices for intelligence gathering purposes. In seeking to balance the Government's obligation to protect the nation with the legitimate right of citizens to maintain their privacy, the number of surveillance devices have been decreased substantially in the past ten years, both in terms of devices in place at any given time and also the total number in use during a given year.

For instance, in 1969, 1970 and 1971, FBI records show that there were never more than 50 wiretaps in operation at any one time, except in two instances, one in 1969 and one in 1970 where authorizations overlapped for a matter of days. Except for those two overlaps, the total number of telephone surveillances has consistently been below 50 for this three year period. Microphone surveillance has never exceeded six at any one time in 1969, 1970 or 1971.

The cumulative total for the year 1970 was 97. In addition, there were a total of 16 microphone surveillances used in all of 1970. From January through October 15 of 1971, there were never more than 43 wiretaps operating at one time, and a total of 79 wiretaps and six microphones for the entire period.

During the 1960-61 period, however, the figures were significantly higher. On February 8, 1961, for instance, there were 145 electronic devices in operation, 78 taps and 67 microphones, according to a Department letter sent to Senator

Ervin's committee. On January 10, 1961, there were 85 wiretaps in operation, Director Hoover said in a letter to the then Attorney General, Robert Kennedy. On the day in 1961 that FBI Director Hoover testified before a Congressional Committee, he said there were 90 wiretaps in operation.

By comparison, there were 32 wiretaps and 4 microphones in operation yesterday in connection with national security matters.

Any assertion that "the total amount of Federal electronic eavesdropping without court permission far exceeds the eavesdropping with judicial approval" is false. The number of court authorized devices in 1970 was 180, compared to 113 national security devices installed.

Court authorized taps, which are used solely for gathering evidence for use in criminal prosecutions, are limited to 30 days' duration. There is no such limit for national security taps, which are solely for the purpose of intelligence gathering. To compare the two for the purpose of drawing inappropriate and preconceived conclusions does not serve the public interest.

INTERVIEW OF RICHARD G. KLEINDIENST BY ELIZABETH DREW ON "THIRTY MINUTES WITH . . ." JUNE 14, 1971

Announcer. "Thirty Minutes With . . . Richard Kleindienst Deputy Attorney General, and Elizabeth Drew.

Miss DREW. Mr. Kleindienst, when your Administration came into office it was very critical of the previous Department of Justice. How do you think what your Department has done in the years it's been in power now differs from the way the old group ran the Justice Department?

Mr. KLEINDIENST. Well, we felt we had a reason to be critical as a result of either the policies of the preceding Administration in the Department of Justice, or probably more accurately, the lack of policies, and I guess, as a self serving statement, we think that we have had policies that have been effectuated and programs that have been put into being that fulfilled a very distinct need and what had come to be a lack in the enforcement of the federal laws in the Department of Justice.

To be specific, I think that the energy, the resources, the personnel and the money that the Congress has been willing to give this Administration and this Attorney General in the field of organized crime, in the field of narcotics, in the field of civil rights enforcement, in the field of antitrust enforcement, have really been remarkable, aggressive steps forward in these vital areas.

If I had to characterize it, again beneficially from the standpoint of this Administration, I think we have been engaged in doing things and less talking about them, and I think perhaps the preceding Administration was doing an awful lot of talk about a lot of things and not too much of the doing.

Miss DREW. Then you feel you've achieved a lot more in these areas—

Mr. KLEINDIENST. Yes, we do.

Miss DREW [continuing]. Besides getting money from Congress.

Mr. KLEINDIENST. Yes, we do. Take civil rights enforcement. I think for political reasons some segments of our society haven't beeen willing to give the President and the Attorney General in this Administration the——

Miss DREW. You mean blacks, don't you? I mean, let's

Mr. KLEINDIENST. Well, I'd say black Democrats, and apparently at this time in our history most of our—the black political leaders are Democrats. But to give this Administration the proper credit that they deserve for increased enforcement in every areas of civil rights enforcement, and then also the miracle of school desegregation in the South of last year without divisiveness, without confrontation, where they in effect, notwithstanding some 15 years following the Brown decision, using the total community, black and white leaders alike, brought an end to our desegregated school districts in the South.

I think the same comparison could be made in organized crime. This Administration, I think through the leadership and the basic strength of Attorney General Mitchell, is now using on cohesive, cooperative, coordinated basis, all of the resources of the federal government: Internal Revenue, the FBI, Customs.

Miss DREW. Well, those strike forces were started by Ramsey Clark, weren't they?

Mr. KLEINDIENST. Yes, they were. There were five strike forces when we came in. There are now 18 or 19, and there will be 23 by the end of this year. But the essential difference is that we have as a matter of committment, when we came in, the full cooperation of all the branches and departemnts of the executive branch of the government, the Tax Division, the Antitrust Division, Internal Revenue, the FBI, Customs, Secret Services, the United States Attorneys' offices, working together in a cohesive way to bring results.

One marked difference, of course, is the fact that this Administration is willing to use court-ordered electronic serveillance in organized crime cases, as a result of which in some 260-approximate such court-ordered electronic surveillances in the last two years we've obtained about 900 indictments in organized crime type situations, and then I think you know that Ramsey Clark, the former Attorney General, absolutely refused to use this technique which was given to the Department of Justice by the Congress.

Miss DREW. Well, that brings up a lot of things that we'll——

Mr. KLEINDIENST. Yes, I'm sure it does [laughing].

Miss DREW [continuing]. That we'll be getting into. I wanted to ask you, and we will get to electronic devices in a few moments, the Attorney General, in talking about the need for the right to use wire taps without court orders, made a speech over the past weekend in which he said, "Never in our history has our country been confronted with so many revolutionary elements determined to destroy by force the government and the society it stands for." I'd like to talk about what he means.

Mr. KLEINDIENST. Well, I think he means that on a relative, comparitive basis in our country today there are probably more—in terms of numbers—subversives, or people who reside in the United States who actively advocate the overthrow of the institutions of our government under the Constitution by either force or violence, or by some other means. As a result of the increased number of such persons—and I'm not talking just about political dissent in a free society. I'm talking about the increased number of persons who advocate the overthrow or the elimination of the government of the United States as we know it under our Constitution.

Miss DREW. How much danger are we in of overthrow of our government?

Mr. KLEINDIENST. Well, I don't think either the Attorney General or I feel that as of right now there is any appreciable danger of our country being overthrown by this number of persons. However, I think that he feels, and I share this opinion myself, that if this government and this society stood by, did nothing, and let the number increase year after year, apparently with the approval of society, that kind of a person who would advocate the overthrow of our government by force or violence or some other means to substitute in place of it a non-Constitutional form of government, we perhaps would arrive sooner than we wish at a point where the threat would be real.

Miss DREW. How do you keep the number from increasing?

Mr. KLEINDIENST. Well, you keep it from increasing, it seems to me, by public debate and disclosure, by being sure that those who actually advocate this kind of conduct are exposed. Secondly——

Miss DREW. Exposed?

Mr. KLEINDIENST. To expose to the public so that you and I and the public know that an individual really is a person who advocates the overthrow of our government. He's not just a person addressing himself to some of the problems of America, problems that all of us are dedicated to solving.

We also feel that when these persons violate the laws that the Congress enacts—and let me provide a footnote there. The only jurisdiction that the Department of Justice has is the enforcement of a valid Constitutional law of the Congress. No other law. It's not laws that we make ourselves, or would like to make ourselves, but it's just the laws of the Congress. Many of those laws of the Congress strike at illegal conduct and activity of persons like this, which constitute in some respects criminal conspiracy. We believe that those persons should be prosecuted if in fact they are violating a federal law on the same basis as the organized criminal or any other type of federal criminal in the United States.

Because some of their conduct strikes at what we call our national security, the basic security of this government, we feel that if it's of that kind that a——

Miss DREW. What sort of conduct is of that kind? That's what I'm trying to understand, is what you think of as a threat to national security.

Mr. KLEINDIENST. Well, maybe I can say it this way, that a person who is a citizen of the United States can engage in conduct which is subversive of our national government in cooperation with foreign agents or foreign countries or foreign ideologies just as much as a citizen of a foreign country who interdicts himself into our country to engage in espionage, and that if a person not only uses his precious first Amendment right of free speech to advocate change or a new philosophy which we think is permissible, but goes beyond that and engages in overt acts of conduct calculated to change our government by non-Constitutional means, by force and by violence, then we feel ——

Miss DREW. Like what?

Mr. KLEINDIENST. Well, to create situations that attack the ability of the government to function at any particular time.

Miss DREW. I mean, would you include Mayday in that definition or are there things beyond that that you'd be concerned about?

Mr. KLEINDIENST. Well, I know that many of the persons—or many persons who were the organizers of the Mayday incident here in Washington, D. C., are persons whose ultimate objective is to overthrow the government of the United States.

Miss DREW. Overthrow——

Mr. KLEINDIENST. By one means or another. The mere fact that they came here to stop the government by what was acknowledged to be, on behalf of the perpetrators of it, illegal conduct I think is an example of what I'm talking about.

Miss DREW. And when you say "overthrow," does that mean that they want to seize power?

Mr. KLEINDIENST. Well, either they want to seize power for themselves or they want to destroy our constitutional government so that other persons who share their belief that the American society and the American government is essentially evil, essentially unable to provide for its citizens, should be eliminated, and that there should be something else put in its place. And what they usually talk about are concepts that they derive from Lenin, from Mao, from Castro, from Che Guevara, from the China—Chinese experiment in Communism. The flags, the slogans, the sayings, the concepts, the ideas seem to suggest that they want to eliminate our form of government, a constitutional government, and substitute for it, a kind of concept of society that is very similar to different forms of communism in the world.

Miss DREW. Do you think they have the power to do it?

Mr. KLEINDIENST. No, I do not. Right now, no, I don't. But I think that it's incumbent upon a constitutional government to use the legal, valid powers conferred upon it by the Congress and approved by the Supreme Court of the United States to deal effectively with that kind of conduct when it arises.

Miss DREW. Now, when the Attorney General made the speech, it was to bolster the Justice Department position that there should be—well, that you should be able to continue to do wiretapping in domestic cases——

Mr. KLEINDIENST. Yes.

Miss DREW [continuing]. Without——

Mr. KLEINDIENST. Just like Ramsey Clark did and Nick Katzenbach and Bobby Kennedy and Bill Rogers——

Miss DREW. Did what? I didn't finish the question.

Mr. KLEINDIENST. Well, electronic surveillance in national security cases.

Miss DREW. In domes—of domestics?

Mr. KLEINDIENST. Yes.

Miss DREW. They did it?

Mr. KLEINDIENST. Oh, yes. Mr. Mitchell, as the Attorney General, acting on behalf of the President, is not engaging in non-court-ordered electronic surveillance of a different order essentially, than any attorney general who proceeded him—and as a matter of fact, statistically is doing less of it. Certainly less of it than Senator Kennedy did when he was the Attorney General. And I believe less than when Mr. Katzenbach was the Attorney General, and just about the same amount as Mr. Clark authorized when he was the Attorney General.

Miss DREW. Well, we're talking about the wiretapping of domestic people held to be a danger——

Mr. KLEINDIENST. American citizens who——

Miss DREW [continuing]. To the national security.

Mr. KLEINDIENST [continuing] Who are engaged in subversive activities and in—thereby endangering our national security.

Miss DREW. Tht's right. And the Attorney General has asserted that power—I thought it was unprecedented what—when he asked for it in the Chicago case.

Mr. KLEINDIENST. No. No, it's not unprecedented.

Miss DREW. And the court of appeals has said that—has ruled it out, said that it—you know, he can't do it. And now it's before the Supreme Court——

Mr. KLEINDIENST. Well, that doesn't mean it's unprecedented. I think every President and every Attorney General since Roosevelt, when they began to use this type of electronic device, because of the advance of electronic engineering, has assumed that they had the power to do it. The Supreme Court, by virtue of either dicta in its decisions or its refusal to hear cases like this, has created the further belief in that assumption and now, for the first time, after these many forty years, the issue will be raised squarely with the Supreme Court. And of course, if the Supreme Court says, "You can't do it," then we won't do it.

Miss DREW. Yeah. Well, to get to my question——

Mr. KLEINDIENST. Oh, I'm sorry, Liz.

Miss DREW. That's all right. Why—what's the problem with going to the courts to get the court order on it?

Mr. KLEINDIENST. Well, superficially you'd say if you have a court order to electronic surveillance in organized crime why not in a case like this?

To begin with, the court really doesn't have the expertise, the background and the facilities to make that kind of judgment, with respect to internal security, the protection of the government. The executive branch can, not because you have a new President who can do it better than another President; but in the executive branch you have a continuation of professional career people whose business it is to understand the whole sensitivity of this issue. That's reason number one.

Reason number two, it seems to me, is that you have some 500 judges, you have thousands of clerks and court personnel. The possibility of a breach of security in cases like this, of extreme sensitivity, both respect to our relations with foreign governments with whom we have diplomatic relations, with respect to the whole business of security, to be sure that innocent persons aren't hurt, and also that—with respect to those that you want to survey—they are not possibly informed about it.

And I think that most people who understand the whole comprehensive nature of this subject matter believe that the executive branch of the government in this kind of case is the proper repository. Now——

Miss DREW. Would there be any limits on it at all?

Mr. KLEINDIENST. Well, sure, there should be some limits, and the Supreme Court, over a period of time will carve and has carved out carefully what those limits are. But there's one additional thing here that Attorney General Mitchell has emphasized, and that is that no such electronic surveillance is authorized except by his personal decision. This fixes direct political and administrative responsibility——

Miss DREW. But we won't know he's doing it if he doesn't go to court. There'll be no way of telling.

Mr. KLEINDIENST. You will know about it—you will know about it because they are a part of the official records of the Department of Justice——

Miss DREW. Could I go in and see the record of who he's——

Mr. KLEINDIENST. No, you could not——

Miss DREW. Okay.

Mr. KLEINDIENST [continuing]. But appropriate persons in the United States Congress can.

Miss DREW. Oh, they can?

Mr. KLEINDIENST. Yes, they can. Now, that does not mean that the executive branch would give out sensitive information, but the Congress has a way and is informed regularly, you know, of the nature——

Miss DREW. Who is being?

Mr. KLEINDIENST. Huh?

Miss DREW. Of who?

Mr. KLEINDIENST. Well, of categories, not exact individuals.

Miss DREW. Well.

Mr. KLEINDIENST. And the interesting thing about it, Liz, is—and I suppose a lot of people in this country think there are thousands of these, you know, authorized wiretaps. And there are a handful, maybe 45, 50, you know. It's a very, very small number. It isn't just hundreds. It isn't thousands. It isn't even dozens. It's a very, very small number.

Miss DREW. When we get to the general question of surveillance, now that the Army has finished its surveillance, or we're told it has, and it's——

Mr. KLEINDIENST. Now, let's talk about the Army, too, for a minute.

Miss DREW. No, I want to talk about the Justice Department.

Mr. KLEINDIENST. The reason why the Army got in it is because President Johnson, as I understood it, couldn't get the kind of information he needed from the Department of Justice, you know, in cases like this. But be that as it may.

Miss DREW. Okay.

Mr. KLEINDIENST. All right.

Miss DREW. You made your point. Now it's——

Mr. KLEINDIENST. (Laughing) That's why I'm here, is to try to make some points.

Miss DREW. It's back—the Justice Department is taking this responsibility now. Who decides who will be surveilled?

Mr. KLEINDIENST. Well, you have two—well, in that kind of situation—your'e talking about this internal security type of surveillance?

Miss DREW. Uh-huh.

Mr. KLEINDIENST.. It comes about or can come about as a result of a recommendation of several persons in the Department of Justice, either Assistant Attorneys General, or staff persons, by way of then formal recommendation documents to the Attorney General. And they, by recommendation only, but he and he only decides it. He does not delegate it to anyone; he has never delegated it to me, or to anyone else. So the Attorney General decides the question himself.

Miss DREW. Now, we—the *Washington Post* had a story over the weekend that there are 10,000 people in what's called a "security index," who would be subject to arrest in case of war or national emergency. Who decides that?

Mr. KLEINDIENST. I read that in the newspaper, and I was rather astounded by it as I——

Miss DREW. You didn't know about it?

Mr. KLEINDIENST. No.

Miss DREW. Really?

Mr. KLEINDIENST. I know that there is some kind of list that has been maintained by the Internal Security Division for decades—the same list that was maintained by Ramsey Clark and Mr. Katzenbach and——

Miss DREW. Yeah. I'm not picking on you for it——

Mr. KLEINDIENST. I've never seen it. I've never been curious about it. I don't know the numbers there.

Miss DREW. And what are you going to do about it now, if you were so amazed by its existence?

Mr. KLEINDIENST. Well, I might get a little curious to find out more about it, but I believe it probably has been a traditional function of the Department of Justice—again, agreed upon by President Roosevelt, Truman, Eisenhower, Kennedy, Johnson and Nixon. I can likewise feel that, since this is the first time, to my knowledge, a story has come out about it, that it's very securely kept under much restraint, for the protection of innocent people. You know, there's rumor information in it.

Miss DREW. Well. But the question would be, who would decide that there was this national security emergency——

Mr. KLEINDIENST. You mean, for the use of a thing like that?

Miss DREW [continuing]. And really, on what grounds these people would be arrested.

Mr. KLEINDIENST. Oh, I can't imagine. You and I have debated this before, but I don't believe people should be arrested and detained without full due process of law. That if you have reasonable cause to believe somebody has committed a crime, arrest him; but if you do, immediately thereafter they should be arraigned, be able to set bail, and then have a trial, you know, very quickly thereafter. I can't imagine—well, it's incomprehensible to me that any

administration, this one, the next one, the next one after that, or past ones, would arrest people and detain them without due process of law. We did it once with the Japanese, which I abhored—did then, have since, and do now. And would never want to see that done again.

Miss DREW. On Mayday, were the——

Mr. KLEINDIENST. Mayday.

Miss DREW. Mayday. Were the arrests there to get the people off the streets or to prosecute them for breaking a law?

Mr. KLEINDIENST. The arrests were there because those policemen under those circumstances, at that time, had reasonable cause to believe that the persons who were at or about the place of activity were either going to commit a misdemeanor or a felony or were in the process of doing so. And I think that's all the law requires, is that reasonable cause at the time.

Now, what happens to them afterward, I think, is a great tribute to our system of due process, because once arrested a person again has to be arraigned within a reasonable period of time. As I recall in the Pentagon disorders of 1967, it took three, four, and five days to have them arraigned, and these people were arraigned and left within 12, 14, 16, 18, 22 hours.

Miss DREW. But I gather it became clear early that evening, or even that afternoon, that there really wasn't enough evidence to prosecute a lot of these people. Why were they held——

Mr. KLEINDIENST. Well, it wasn't——

Miss DREW [continuing] In the camps?

Mr. KLEINDIENST. It wasn't clear, Liz. It wasn't clear until you could create a situation where once a person was arrested, he was properly arraigned, whether a policeman was available under the circumstances, to come into court and identify that person and say, "Yes, I saw him at 6:45 a.m. this morning throw a can out in the street or resist arrest or not move along." In each case, when there wasn't such an identifying police officer, the case was dismissed, as it should have been.

Miss DREW. But that was known that night——

Mr. KLEINDIENST. But you couldn't——

Miss DREW [continuing]. Wasn't it, that there wasn't——

Mr. KLEINDIENST. You couldn't predetermine each case, however, until you've gone through them all. You don't let—you—I think that you have the obligation to go ahead and finish due process——

Miss DREW. For the whole group.

Mr. KLEINDIENST [continuing]. Which you do in every case. For the whole group. Yes, indeed.

Miss DREW. Even though it was clear that you didn't have the evidence on them all?

Mr. KLEINDIENST. Well, sure, but how do you know which ones until the process has worked itself out? The great thing about this whole situation is—and that is, to my knowledge, no innocent person has been convicted, you know, of wrongful——

Miss DREW. Hardly anyone's been convicted——

Mr. KLEINDIENST. Well, fine. But that also means there have been no innocent people convicted. If the law had to be sure that a person was guilty before he was arrested, you would never have anybody arrested under our system of jurisprudence. What we are interested in is to see that no innocent person is convicted of a crime that he did not commit.

Miss DREW. But does this mean that when you have large groups in town again, I mean, that they might expect that this same procedure again——

Mr. KLEINDIENST. Well, there's—large groups have been in this town before, six times since I've been the Deputy Attorney General——

Miss DREW. Well, some of which are interfering with——

Mr. KLEINDIENST. This is the first time a large group apparently conspired to stop the government by illegal conduct and activity. And it was illegal conduct and activity. I don't think, and I certainly hope, that that kind of group will come back and try to do that again. If they did it again under these circumstances as existed before, I would fully expect, I would urge, that the same steps be taken as was taken by Chief Wilson on that day.

Miss DREW. I have a lot of subjects I want to cover, and you're out-talking me. We're not going to get through——

Mr. KLEINDIENST. [Laughter.]

Miss DREW. [Laughing] We're not going to get to them all, but one I wanted to ask you about is gun control. Do you think that people should be permitted to have handguns?

Mr. KLEINDIENST. Well, some people should and some people shouldn't. I essentially——

Miss DREW. What about a law against handguns? That's around.

Mr. KLEINDIENST. Well, I essentially believe that, with the exception of a few areas of this, that that is a matter for state and local authorities.

Miss DREW. Why?

Mr. KLEINDIENST. The handgun situation is one thing in New York City than it is in Idaho or Nevada or another area. I think that there is some legitimate part to play for the federal government, but I don't think it's the kind of situation where you want to run in and have a federal response to it.

Secondly, I think it would be almost impossible to go out and confiscate every gun in the United States. If people of a criminal bent wanted to keep guns, they would. There's also a legitimate interest on behalf of the law-abiding person to use guns for hunting.

Miss DREW. Now, I'm talking about handguns, not rifles.

Mr. KLEINDIENST [continuing]. Or for recreational support. I'm talking about handguns. I'm talking about——

Miss DREW. Handguns for hunting?

Mr. KLEINDIENST. Sure, for recreation. Not hunting on handguns, but for recreation——

Miss DREW. Well——

Mr. KLEINDIENST. And then, I think there's also an interest in—on behalf of an individual citizen to be able to have a handgun in his house for his own self-protection. So that when you start weighing all of the interests, I think it's pretty difficult to urge a comprehensive, standard, federal solution to this problem; and I think the Congress has rejected that. I think that they turned that approach down.

Miss DREW. Senator Kennedy was here last week, and I—he was talking about this, and he said that the reason this Administration doesn't come out for this kind of control is it's overly influenced by the National Rifle Association. Do you have any response to that?

Mr. KLEINDIENST. Well, I'd hate to comment about the groups that overly influence Senator Kennedy.

Miss DREW. Well, go ahead. He talked about you.

Mr. KLEINDIENST. Well, I think—I don't think that the National Rifle Association overly influences this administration.

Miss DREW. Excuse me. He really didn't say "overly." I did that wrong. He said, "influenced."

Mr. KLEINDIENST. I think the position taken by the President on this subject matter is consistent with the position that he took in the campaign, and I wish Senator Kennedy would be as forthright in campaigns as President Nixon has been. And then thereafter be consistent in his—in his role as a senator, you know, about the things he said in campaigns. There's nothing inconsistent about this Administration's campaign posture on gun control, than it has backed up since it's been here, and I personally think it's the correct position.

Miss DREW. Well, I don't know that you answered me, but that's all right. We just have a couple of minutes left, but I wanted to get in a little bit about your own background. You grew up in—what was it? Winslow, Arizona?

Mr. KLEINDIENST. Winslow, Arizona, uh-uh. A little town, a little railroad town in the northeastern part of Arizona. My grandfather homesteaded there in 1909. He had been born in Washington, D. C., as a matter of fact.

Miss DREW. And then you—you went to Harvard, didn't you?

Mr. KLEINDIENST. Well, I did a lot of things before I got to Harvard. I did a lot of dishwashing and automobile mechanic work. I was a cook and a waiter. I was at the University of Arizona for a year before World War II, I was in the service, and then transferred to Harvard College after World War II, in 1946. Then I went to the law school, and when I graduated from law school, I went back to Phoenix, where I practiced law for twenty years.

Miss DREW. You know, the—we were talking about wiretapping before, and as you know, a lot of people—as you said, people think more is going on than is. And a lot of people think their phones are being tapped, and——

Mr. KLEINDIENST. Uh-huh. I know it, and that's a bad thing in a free society, you know.

Miss DREW. Well, that's what I wondered—wanted—if that bothers you, that that's going on now.

Mr. KLEINDIENST. It bothers me, but——

Miss DREW. Why do you think they're so—they feel that way?

Mr. KLEINDIENST. Well, I think some politicians are trying to exaggerate the problem for strictly political purposes, and politicians who should know better. Because the general policies of the Attorney General under Presidents Eisenhower, Kennedy, Johnson, and Nixon, has been almost the same. And yet I think it's for political reasons that the matter has become one of hysteria right now. When it could just as easily have been that when you had Democratic Presidents.

And I think it's been for political reasons that some politicians, the Democratic Party, who seek to defeat President Nixon, are trying to make—or manufacture an issue out of it. If they were as sincere two or three years ago as they are now, they could have done it then. So I therefore attribute it to political motives.

Miss DREW. You know, there is a sort of fear, really, I guess would be the right word——

Mr. KLEINDIENST. By some.

Miss DREW. Well, I was about to say something else—of this Justice Department. How does that make you feel, to be part of something like that——

Mr. KLEINDIENST. Well——

Miss DREW [continuing]. Whether it's valid, or not. It's there.

Mr. KLEINDIENST. Well, so long as I know that it's not valid, it doesn't bother me. I'm disturbed that—that anybody would create false impressions about me or the Attorney General in this area. We feel that we're very careful, we're very moderate men. We—all of the men in this Department are trained lawyers, that was our career before we got there, it's going to be our career when we leave. And if you are a good lawyer in a free society, you take very seriously the guarantees of the Constitution, the rights of individual citizens; you're very jealous in guarding civil liberties——

Miss DREW. We're out of time, I'm sorry. Get—two more words.

Mr. KLEINDIENST. Are we out of time?

Miss DREW. We are out of time. Thank you very much.

Mr. KLEINDIENST. I was just getting warmed up, Liz [laughing].

Miss DREW. Come back. Let's go on. Thank you very much.

Mr. KLEINDIENST. Thank you.

EXCERPT FROM INTERVIEW WITH ATTORNEY GENERAL JOHN MITCHELL, ON "THE DAVID FROST SHOW", April 7, 1971

* * * * * * *

FROST. Welcome back. Talking with Attorney General John Mitchell. Everybody gets very worried by the phrase, "electronic surveillance," and sees 1984 just around the corner. Electronic surveillance really means two things, doesn't it? Wiretapping and bugs. How much, really, is there going on at the moment?

MITCHELL. Well, if I can put this into context, because there are different facets to it. There are really three facets to it. Number one is the court-authorized electronic surveillance that we have been using against organized crime and kidnapping and counterfeiters, and so forth. I believe that, since we have come into office in January of 1969, there have probably been up to date about 300 of those, most of which of course are wiretapping. And of course we have to file a complete report in the federal establishment, with everything, including how much it costs us to do it. We have never had a single complaint from anybody about that.

The second aspect of it, of course, is what we refer to as the national security area, in which we exercise, or at least I do, under the direction of the President, the same powers that have been exercised by very Attorney General and President since they invented the system. And I can say right here and now that we have used it less than some of our predecessors in office. And I would also say that this nonsense of some of these paranoid people that think that the Congressmen or Senators are being bugged or they hear a click on their phone and they think they're being bugged is just absolutely nonsense.

FROST. That's just the phone company, is it?

MITCHELL. That's the bad wiring, or what ever it may be.

Now, the other aspect of it I'd like to point out, that in this legislation of 1968 that we are using we now in the federal government have a handle of getting at individuals in the private sector and unauthorized local police forces, and so forth, which were using electronic surveillance, wiretapping and the rest of it. And we have quite a number of prosecutions. So that I would say that, far and away, since this legislation and since the activities are carried on as I have described them, there is much less likelihood of an individual being wiretapped than there ever was befored, because of our prosecutions of the private detectives and the rest of them that had been using it over the years.

FROST. In the two areas where you do operate, and the area one, in chasing criminals of one sort or another, how many of those—309, is it, since you've come into office?

MITCHELL. Well, they go on—it's slightly over 300, I believe, at the last reporting or counting. But they go on from day to day; the number will change. And of course they are put on for a limited period of time. Most of them are 15 days. The maximum is 30 days. And if you want to use it longer in some big racket operation, you'd have to go back to court and get an extension on it.

FROST. And are there more or less in section two, in the area of national security?

MITCHELL. More or less than what?

FROST. More or less than in the first area, more or less than 300?

MITCHELL. Oh, no, no, no, no, no. Much, much less. There are less than 50 of them.

FROST. Less than 50?

MITCHELL. Oh, yes, yes. And there again, of course, they relate to particular subject matters at a particular time.

FROST. I see. And how long do they run for? They can run indefinitely?

MITCHELL. Well, they could run indefinitely, but of course in most cases that would be entirely nonproductive because—I hasten to point out that what we are looking for is intelligence that we need for the security of this country. And so that it isn't appropriate in most cases to just put on a wiretap and leave it there.

FROST. What is the exact number? It is much under 50 at the moment?

MITCHELL. It's never been disclosed.

FROST. It's never been disclosed. But when you said it's less—well, it's less than 50, and that is less than some previous administrations.

MITCHELL. Yes, considerably so.

FROST. It went much higher, then. But I mean I presume a lot of the material—as you say, you want intelligence. A lot of material you must get from a wiretap is, "Could you send around two pounds of butter" and lots of—I mean how many people does it need to operate one wiretap?

MITCHELL. It doesn't need anybody. It's all done automatically, if you want it done that way.

FROST. But I mean how many people are needed to listen to everything? I mean do you need six people per wiretap or . . .

MITCHELL. No, it depends on, of course, where the tap is and where the phone is used and how it's used and so forth.

* * * * * * *

[From the New York Times, June 12, 1971]

MITCHELL UPHOLDS WIRETAP OF "DANGEROUS" RADICALS

(By Fred P. Graham)

WASHINGTON.—Attorney General John N. Mitchell said today that "never in our history has this country been confronted with so many revolutionary elements determined to destroy by force the Government and the society it stands for."

In a speech in support of the Nixon Administration's contention that it can wiretap "dangerous" radicals without court approval, Mr. Mitchell declared that "the threat to our society from so-called 'domestic' subversion is as serious as any threat from abroad."

He made the statements as he gave his most detailed legal argument thus far in support of the Administration's assertion that the threat from foreign and domestic elements was indivisible, and that the President had the authority to wiretap both without court authority.

Lawyers inside the Government and out expressed surprise that Mr. Mitchell would take this legal issue to the people as he did today in a speech and a press release, because the question is now before the Supreme Court in the form of an appeal by the Justice Department.

REJECTED BY APPEALS COURT

The United States Court of Appeals for the Sixth Circuit rejected the Administration's argument last April, ruling that when the Government wished to wiretap domestic groups, it must obtain judicial approval. Asserting that that decision was wrong, the Justice Department has asked the Supreme Court to review it.

In the past, when matters have been pending before the Supreme Court, Justice Department officials have avoided making statements that might be regarded as exerting pressure upon the justices.

Mr. Mitchell's statements were made in a 15-page speech prepared for delivery tonight before the Virginia Bar Association in Roanoke. It was released this afternoon by the Justice Department's press office, together with a three-page press release that quoted Mr. Mitchell as specifically disputing the Appeals Court ruling.

The press release characterized Mr. Mitchell's speech as asserting that such wiretapping "meets the constitutional test of reasonable search and seizure and that such surveillance is necessary to permit the President to fulfill the obligations of his office."

PRESIDENT'S DUTY

In his speech, Mr. Mitchell based his case on the President's constitutional duty to protect the country.

"Were the President to permit the overthrow of [the] Government by unconstitutional means, he would be violating his constitutional oath," he said.

"The Constitution of the United States cannot possibly be construed as containing provisions inconsistent with its own survival. It is the charter for a viable government system, not a suicide pact."

He asserted that there was no dividing line between hostile foreign forces and domestic elements seeking to overthrow the Government. Domestic subversives are "ideologically and in many instances directly" connected with foreign interests, he said. If it were possible to separate the two, he added, "history has shown greater danger from the domestic variety."

Mr. Mitchell said that surveillance of such groups was not affected by a 1967 Supreme Court decision, Katz v. United States, that held that wiretapping was covered by the Fourth Amendment's prohibition against unreasonable searches and seizures, and that the police must obtain wiretap warrants before using eavesdropping devices.

He argued that it was not unreasonable to wiretap subversives or suspected bombers. The distinction to be drawn, he said, is not whether the subjects are foreign or domestic, but whether the wiretaps are used for "intelligence" or prosecution purposes.

When they are used to gather intelligence, and the information is not to be used in court, he said the President and his officials were in a far better position to know if a device should be installed than the Federal judges across the country.

"You cannot separate foreign from domestic threats to the Government and say that we should meet one less decisively than the other," Mr. Mitchell said. "Either we have a constitutional Government that can defend itself against illegal attack, or in the last analysis we have anarchy."

[From the Nation, June 14, 1971]

Misleading The Presidents—Thirty Years of Wire Tapping

(By Athan G. Theoharis)

[*Mr. Theoharis, associate professor of American history at Marquette University, is the author of* Seeds of Repression: Harry S. Truman and the Origins of McCarthyism (*Quadrangle Books*) *and* The Yalta Myths: An Issue in American Politics, 1945-55 (*University of Missouri Press*). *The research for this article, in which Mr. Theoharis was assisted by Paul Quirk of Marquette University and Lynn Parsons of Wayne State University, was supported financially by the Truman Institute for National and International Affairs.*]

The history of government use of wire tapping, particularly during the early years of the Truman Presidency, provides one reason for concern over White House-Justice Department relations. In 1940, responding to the outbreak of war in Europe and the subversive role played during the 1930s by Fascist parties in France, Austria and Czechoslovakia, the Roosevelt administration supported legislation to legalize wire tapping in "national defense" cases. At that time Rep. Emanuel Celler (D. N.Y.) had introduced a bill that would have amended section 605 of the Communications Act of 1934 and permitted the FBI, subject to the approval of the Attorney General, to wire tap in cases involving interference or attempts to interfere with the national defense by sabotage, espionage, conspiracy, violation of the neutrality laws, or "in any other manner." Information thus obtained was to be admissible as evidence. The Congress failed to enact the legislation and, lacking legislative authorization, President Roosevelt on May 21, 1940 issued instead an executive order stipulating:

> I have agreed with the broad purpose of the Supreme Court decision [in *Nardone*] relating to wiretapping in investigations. The Court is undoubtedly sound both in regard to the use of evidence received over tapped wires in the prosecution *of citizens* in criminal cases; and it is also right in its opinion that under ordinary and normal circumstances wiretapping by government agents should not be carried out for the excellent reason that it is almost bound to lead to abuse of civil rights.
>
> However, I am convinced that the Supreme Court never intended any dictum in the particular case which it decided to apply to grave matters involving the defense of the nation.
>
> It is, of course, well known that certain other *nations* have been engaged in the organization of propaganda of so-called "fifth columns" in other countries and in preparation for *sabotage*, as well as in active sabotage.
>
> It is too late to do anything about it after sabotage, assassinations and "fifth column" activities are completed.
>
> You are, therefore, authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigating agents that they are at liberty to secure information by listening devices direct to the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies. *You are requested furthermore to limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens.* (Emphasis added.)

With the end of World War II and Harry S. Truman's accession to the Presidency, the issue of continuing this directive came into question. In July 1946, Tom C. Clark, Truman's Attorney General, pressed the President to continue the wire-tapping authorization. Exploiting Truman's anxieties about deteriorating U.S.-Soviet relations, the active role of the U.S. Communist Party in civil rights and labor activities, and recent disclosures of subversion or lax security procedures, Clark wrote the President on July 17, 1946:

> Under date of May 21, 1940, President Franklin D. Roosevelt, in a memorandum addressed to Attorney General Jackson, stated:
>
> "You are, therefore, authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigating agents that they are at liberty to secure information by listening devices direct to the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies."

> The directive was followed by Attorneys General Jackson and Biddle, and is being currently followed in the Department. I consider it appropriate to bring the subject to your approval at this time.
>
> It seems to me in the present troubled period in international affairs, accompanied as it is by an increase in *subversive activities here at home*, it is as necessary as it was in 1940 to take the investigative measures referred to in President Roosevelt's memorandum. At the same time, the country is threatened by a very substantial increase in *crime*. While I am reluctant to suggest any use whatever of special investigative measures in *domestic* cases, it seems imperative to use them in cases *vitally affecting the domestic security*, or where human life is in jeopardy.
>
> *As so modified*, I believe the outstanding directive should be continued in force. If you concur in this policy, I should appreciate it if you would so indicate at the foot of this letter.
>
> In my opinion, the measures proposed are within the authority of law, and I have in the files of the Department materials indicating to me that my two *most recent predecessors* as Attorney General would concur in this view. (Emphasis added.)

While implying that this new directive would be a simple extension of Roosevelt's policy, and thereby reducing any suspicions that Truman might have held about wire tapping and the relationship of this policy to that of his predecessor, Clark had significantly distorted the Roosvelt directive. In his quote from the operative paragraph of Roosevelt's directive, Clark had deleted its last qualifying sentence—"You are requested furthermore to limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens." Moreover, Clark's letter did not convey the essence of the Roosevelt memorandum, whether Roosevelt's concern about the abuse of this authority or his restriction of wire tapping to foreign activities involving sabotage. In addition, Clark's intent went significantly beyond Roosevelt's, in that he proposed that wire tapping be used to investigate domestic crime or "subversive" activities. In the absence of good staff work that would have apprised him of the specific nature of Roosevelt's policy, and accepting the assurances of his Attorney General, Truman signed the letter. By so doing, he provided the basis for a significant change in executive wire-tapping policy.

The manner by which this extension was secured reveals much about the relationship of the President and his Attorney General and the effective control that an executive exercises over his subordinates. Subsequent developments raise questions about Justice Department use of public relations. Thus, when popular concern about FBI wire tapping arose in the Judith Coplon case in 1949 and again in 1950, the Department of Justice sought through press releases to convey the impression not only that wire tapping was tightly controlled and restrained, but that the basis for this authority derived from President Roosevelt. In March 1949, Attorney General Clark maintained that FBI wire tapping had occurred only "in limited cases with the express approval in each individual instance of the Attorney General. There has been *no new* policy or procedure since the *initial* policy was stated by *President Roosevelt* and this has continued to be the Department's policy whenever the security of the nation is involved." (Emphasis added.)

Knowing how wire tapping was extended and publicly justified during the Truman years is sufficient reason for requiring that the legislature delineate specifically the limits to executive "national security" uses of the technique. As matters stand, there is assurance neither that the President will use wire tapping with restraint nor that he will be fully apprised of procedures instituted within his own administration. The complexity and far-reaching responsibilities of the modern Presidency have increased the possibility that the Chief Executive will not be fully informed about the basis for policy decisions or the procedures of his subordinates. Necessarily dependent for advice and information on nonresponsible subordinates, a cold-war President is vulnerable to being manipulated and, beyond that, to mainipulating the Congress and the public. The corruption inherent in unlimited grants of power requires that traditional processes of control be established, that the simple affirmation of "national security" not remove constraints that would limit abuse or specifically delineate executive authority.

In this sense, the language of Title III of the Omnibus Crime Control Act of June 1968 is too vague to provide the safeguards that national policy requires.

Moreover, when formulating and debating the Act, Congress failed to fulfill its legislative responsibilities and let references to "national security" avert the necessary consideration of Presidential powers and uses of wire tapping. This authorization of wire tapping by federal, state and local law-enforcement agencies demands careful scrutiny as to its constitutionality, wisdom and necessity. Most important, it must be determined whether a simple claim of "national security" seriously restricts the liberties of non-conformists, radicals or dissenters. In this article, I shall discuss the "national security" provision of Title III of the Omnibus Crime Control Act of 1968; the related question of the constitutionality of wire tapping in criminal cases will not be treated.

The major themes of the debate over this authorization were immediately outlined when Ramsey Clark, incumbent Attorney General, after passage of the Act and during testimony before the Senate Appropriations Committee, expressly opposed wire tapping as a general tool of law enforcement. It was not necessary, Clark affirmed, in criminal investigations; constitutional limitations made it virtually useless as a method of crime detection. More effective law enforcement at the local level was the best means to prosecute crime. Consistent with this position, Clark refused to employ the broad grant of authority provided by the Act, restricting federal use to national security cases.

John Mitchell, Clark's successor, does not share this aversion; he has expressed his intention to utilize the authority provided by the Act. His statement of Justice policy, particularly enunciated in a brief filed in Chicago Federal District Court and released in Washington on June 13, 1969, outlined the general objectives and methods of departmental wire-tapping policy. In this brief, the Attorney General maintained that the Department of Justice had legal power, without court approval, to eavesdrop on members of organizations it believed intended to "attack or subvert the Government by unlawful means." Mr. Mitchell further acknowledged that the Justice Department had instituted wire taps on four of the eight defendants in the Chicago conspiracy trial. Outlining the justification for this action, the brief contended:

> There can be no doubt that there are today in this country organizations which intend to use force and other illegal means to attack and subvert the existing form of government. Moreover, in recent years there have been an increasing number of circumstances in which Federal troops have been called upon by the states to aid in the suppression of riots. Faced with such a state of affairs, any President who takes seriously his oath to "preserve, protect and defend the Constitution" will no doubt determine that it is not "unreasonable" to utilize electronic surveillance to gather intelligence information concerning these organizations which are committed to the use of illegal methods to bring about changes in our form of government and which may be seeking to foment violent disorders. . . .
>
> The question whether it is appropriate to utilize electronic surveillance to gather intelligence information concerning the activities and plans of such organizations in order to protect the nation against the possible danger which they present is one that properly comes within the competence of the executive and not the judicial branch.

The vagueness of this policy statement, the implication that wire tapping would be used for domestic surveillance—without court authorization, at the sole discretion of the executive branch and with no heed either to the prohibitions of the Fourth Amednment or to the court-approved requirements of Title III of the Omnibus Crime Control Act—heightened fears within the legal profession and among certain liberal and radical organizations. This alarm coincided with further disclosures about Justice Department and FBI investigative activities. At about the time of the passage of the 1968 Act, it became known that the FBI had wire tapped not only the Chicago conspiracy trial defendants but also Joe Namath, Mohammed Ali, Dr. Martin Luther King, Jr., Stokely Carmichael, Elijah Muhammad, the Black Panthers, certain anti-war groups, H. Rap Brown, Roy Cohn, Dr. Benjamin Spock, and the other defendants in the Boston draft case. Indeed, one civil libertarian, commenting on the extent of this use, feared that: "Given the nature and manifestations of unrest in our cities, there is a real possibility that eavesdropping could be employed to control the protests of the poor and their supporters who petition for redress of grievances."

In response, the ACLU on June 26, 1969 filed a suit in the U.S. District Court in Washington on behalf of nine anti-war and Black Power organizations

and the eight defendants in the Chicago conspiracy trial. Seeking to ban electronic surveillage of political dissenters, and citing the Justice Department's June 13th brief and its implied use of "national security" to justify surveillance of dissident political groups, the ACLU brief condemned Attorney General Mitchell and FBI Director Hoover for having "assumed judicial, penal and otherwise regulatory control over the protesting activities of all dissenting Americans," and for their announced policy of "unfettered executive power to determine possible danger."

The concern motivating the ACLU suit seemed to be confirmed by a subsequent *New York Times* story reporting the response of Nixon Administration aides to recent bombing incidents. On April 12, 1970, the *Times* reported that these unidentified aides viewed the occurrence of domestic bombings as posing a serious internal security threat that required electronic surveillance. One of them remarked to the *Times* correspondent that had the FBI put a tap on the phone of Diane Oughton, who was killed in a Greenwich Village bomb explosion, it might have been able to arrest her before the bomb exploded The *Times* writer wondered whether the Administration was making a case for greater surveillance of domestic radicals.

The fear that wire tapping can amount to poltical surveillance of radicals and dissenters leads one to examine the broad authority granted by the Omnibus Crime Control Act. Section 2511, Title III stipulates:

> Nothing contained in this statute or in section 605 of the Communications Act of 1934... shall limit the *constitutional* powers of the *President* to take such measures as *he deems necessary* to protect the Nation against *actual* or *potential* attack or *other hostile acts* of a foreign power, to obtain foreign intelligence information *deemed* essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything in this chapter be deemed to limit the *constitutional* power of the President to take such measures as *he deems necessary* to protect the United States against the overthrow of the Government by force or *other unlawful means*, or *against any other clear and present danger to the structure or existence* of the Government. The contents of *any* wire or oral communication intercepted by *authority of the President* in the exercise of the foregoing powers may be received in evidence... only where such interception was *reasonable*, and shall not be otherwise used or disclosed except *as is necessary* to implement that power. (Emphasis added.)

The majority report of the Senate Judiciary Committee, issued on April 29, 1968, stressed the same themes. Its language did nothing to define more precisely the limts to executive wire-tapping authority in the realm of "national security." While emphasizing the need to prohibit unauthorized use of wire tapping and to prevent its abuses, the report nonetheless added:

> It is obvious that *whatever* means are necessary should and must be taken to protect the national security interest. Wiretapping and electronic surveillance are *proper* means for the acquisition of counterintelligence against hostile actions of foreign powers. *Nothing* in the proposed legislation seeks to disturb the power of the President in this area. Limitations that might be deemed proper in the field of *domestic affairs* become artificial when international relations and *internal security* are at stake.

The report further emphasized:

> Paragraph (3) is intended to reflect a distinction between the administration of domestic criminal legislation not constituting a danger to the structure and existence of the Government with the conduct of foreign affairs. It makes it clear that *nothing* in the proposed chapter or other act amended by the proposed legislation is intended to limit the *power of the President* to obtain information by *whatever* means to protect the United States from the acts of foreign powers including acutal or *potential* attack of foreign intelligence activities, *or any other danger to the structure or existence* of the Government. When foreign affairs and *internal security* are involved, the proposed system of court ordered electronic surveillance envisioned for the administration of domestic criminal legislation *is not intended necessarilly to be applicable*.... The *only* limitation recognized in this use is that the interception *be deemed reasonable based on an ad hoc judgment taking into consideration all of the facts and circumstances of the individual case.* (Emphasis added).

Although the implication of the language of the report and of Title III was that this broad grant of authority was based on the President's constitutional prerogatives and was intended simply to meet a foreign threat, particularly foreign intelligence, the qualifying references to "internal security" and "other danger to the structure or existence of the Government" could be used to authorize surveillance of radical anti-war, Black Power, or socialistic groups. Seeking to quell fears of domestic surveillance, the bill's proponents contended that the authorization was tightly defined, that use of it would be restrained and consistent with constitutional and libertarian principles.

Indeed, the majority report of the Judiciary Committee abounds with reassuring phrases. With the exception of "duly authorized" law-enforcement officials inevstigating "specified type of crimes" pursuant to prior court order, wire tapping was prohibited. Indeed, one reason for the proposed legislation was the threat posed by scientific and technological developments in electronic surveillance. Authority for wire tapping was "carefully circumscribed." "[T]he *Berger* and *Katz* decisions [were used] as a guide in drafting Title III... [which] has as its dual purpose (*1*) protecting the privacy of wire and oral communications, and (*2*) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized."

The language of the Act contained the same assurances. This legislation was intended to prevent wire tapping "without legal sanction" and "to define on a uniform basis" the circumstances and conditions where it would be authorized. Electronic surveillance would be permitted only "when authorized by a court of competent jurisdiction" and would be limited to "certain major types of offenses and specific categories of crime with assurances that the interception is justified and that the information obtained thereby will not be misused." A thirty-day limit was imposed on each tap, although this authority was renewable. Exceptions to the obtainment of a court order were permitted for reasons of "national security" or where an "emergency situation" required immediate action. In the latter case, law-enforcement officials were allowed to tap for a forty-eight-hour period before being required to secure court appproval. Finally, a National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Eavesdropping was to be established and given responsibility to review the use and operation of the law. The commission was specifically directed to report its findings to the President and Congress.

During the Senate debate on the proposed bill, Sen. John McClellan (D., Ark.), the floor manager of the bill, also emphasized that the "first major purpose of the Title III is to protect privacy of communication." The bill, McClellan added, "has been carefully drafted to meet both the letter and spirit of the constitutional tests set out in *Berger* and *Katz*. Electronic surveillance is authorized but only under strict controls. Broadly, Title III creates a court order system of electronic surveillance. . . . Approval may be given only under certain carefully detailed conditions. . . . It clearly and narrowly assures that electronic surveillance is intended to be the exception, rather than the rule. It is envisaged that these techniques will be employed in only limited numbers and kinds of criminal investigations. On the federal level, the two chief areas are national security matters and organized crime. The specific offenses are designated in the statute. Finally, Title III sets out a series of detailed reporting requirements."

This rhetorical disparagement of unwarranted fears of "Big Brother" was continued after 1969 in public statements by the Nixon Administration and Senator McClellan. The use of wire tapping, both maintained, was restrained; the number of taps was numerically insignificant. In a June 19, 1969 press conference, moreover, President Nixon described his Administration's wire-tapping policy as being "that it should be used very sparingly, very carefully—having in mind the rights of those who might be involved—but very effectively to protect the internal and external security of the United States." A House Republican Task Force on Crime, Atty. Gen. John Mitchell, and Deputy Atty. Gen. Richard Kleindienst similarly emphasized the care to be exercised.

And, in a series of press releases, the Justice Department reported the number of court-approved wire taps in use as being 54, 31, 70, 33. These varying figures, however, referred only to court-approved wire taps which had been terminated and did not include "national security" taps. The release, and news

stories based on it, did not emphasize the distinction, and the low figures cited seemed to bespeak great caution and minimal use.

Senator McClellan and others in the Senate iterated this contention, while at the same time extolling the successes of Administration use of wire tapping. Disclosing that the Justice Department had reported using wire taps or electronic surveillance in 133 cases in the eighteen-month period since the Nixon Administration had assumed office, McClellan praised the effective use of this technique. He cited the number of indictments, arrests and convictions made possible by taps, and observed that Attorney General Mitchell had personally studied each request before authorizing application for court approval. The Justice Department, McClellan emphasized, had made a total of 137 court requests, only one of which had been denied, and had used the court authorization in every case but three. However, McClellan's analysis, like the Justice Department's press releases, failed to mention the extent of departmental usage in "national security" cases; nor did it discuss how the President and his Attorney General defined either the executive's "constitutional" powers or threats to the "structure or existence" of the government.

Accordingly, both the constitutionality and the extent of departmental use of wire tapping, outlined in the June 13, 1969 brief, require a determination of the nature of and legitimacy for the authority granted under the Omnibus Crime Control Act. The Act itself—in contrast with McClellan's assurances during Senate debate and the majority report's emphasis—does not define the limits to executive authority. The Act and the report virtually cede to the President unchecked latitude on "national security" grounds, clearly approving an extensive use, though qualifying this grant by references to "constitutional" powers or "reasonable" purposes. The opportunity of Congressional debate, since specific amendments were offered to Title III of the Senate bill (S. 917) and formal opposition was led by Sens. Philip Hart (D., Mich.) and Edward Long (D., Mo.), should have delineated what powers and latitude, what limits to executive authority, the Congress intended to convey by this legislative grant. Presumably, this debate would have made evident whether the June 13, 1969 brief was consistent with the 1968 Act and with the limitations the Congress recognized to the constitutional powers of the President.

In their minority report, Senators Long and Hart contended that Title III was "unconstitutional, as it provides for unreasonable searches and seizures." Hart maintained in addition that section 2511 (3)—"against any clear and present danger to the structure or existence of the Government"—left too much discretion to a President:

> Under 2511 (3) a President on his own motion could declare a militant right wing group (i.e., the Minutemen) or left wing group (i.e., Black Nationalists), a national labor dispute, a concerted tax avoidance campaign, draft protesters, the Mafia, civil rights demonstrators, a "clear and present danger to the structure of the Government." Such a declaration would allow unlimited unsupervised bugging and tapping. . . . As drafted . . . Section 2511 (3) gives the President a blank check to tap or bug without judicial supervision, when he finds, on his own motion, that an activity poses a "clear and present danger to the Government."

During Senate debate on Title III, Hart again raised the point. The language of the bill as drafted, he argued, failed to provide limits to executive authority or to delineate the basis for the national security exception. Hart's speech drew a response from Senators McClellan and Spessard Holland (D., Fla.) over the meaning of the bill's language. The issues raised in this extended debate, and the specific responses of McClellan and Holland to Hart's queries, because important for an understanding of Congressional intent, warrant extensive quotation.

Introducing the discussion on the meaning of section 2511 (3), Hart maintained that, as he read the language, the President would be authorized to declare that the Black, Muslims, Ku Klux Klan, draft dodgers, or civil rights advocates constituted a clear and present danger. Hart continued, "If that is the case, section 2511 (3) grants unlimited tapping and bugging authority to the President. And that means there will be bugging in areas that do not come within our traditional notion of national security." Hart then pressed McClellan as to whether this reading of section 2511 (3) was a fair one.

In reply, McClellan evasively stated, "This language is language that was approved and, in fact, drafted by the Administration, the Justice Department.

I have not challenged it. I was perfectly willing to recognize the power of the President in this area. If he felt there was an organization—whether black, white or mixed, whatever the name and under whatever auspices—that *was plotting to overthrow* the government, I would think we would want him to have the right." McClellan further maintained that it was not necessary to define the President's powers and, moreover, that the language coincided with the "spirit of permitting the President to take such action as *he deems necessary when the government is threatened.*" (Emphasis added.)

As defined by McClellan, the bill permitted surveillance of groups or individuals planning overt revolutionary acts; it presumably did not include radical politics as such. However, the distinction was not made explicit in the bill or in the majority report, being left to the discretion of the President. Accordingly, Hart pursued this matter further, seeking to determine what McClellan understood the President's constitutional powers to be and what limits he recognized to Presidential action in the national security area. Hart asserted, "If, in fact, we are here saying that so long as the President *thinks* it is an activity that constitutes a clear and present danger to the structure and existence of the government, he can put a bug on without restraint, then clearly I think we are going too far." Responding to this statement, Senator Holland deemed Hart "unduly concerned about this matter." The section to which Hart referred did not "affirmatively" give any power to the President, but simply stated that Presidential power was not restricted. "There is *nothing* affirmative in the statement." McClellan concurred.

Conceding that the Congress could not extend Presidential powers, Hart nonetheless maintained that the language of the section as drafted did not define the limits of the President's national security power under present law. "As a result of this exchange," he added, "I am now sure no President, thinking that just because some political movement in this country is giving him fits, *he could read this as an agreement from us that, by his own motion, he could put a tap on.*" There was not "a single indication that anything affirmative is being done," Holland reiterated; but the Congress was not foolishly seeking to "negate" the constitutional powers of the President.

This exchange, combined with the unsuccessful efforts by Senators Hart and Long to secure Senatorial approval of amendments to clarify the language of the bill and to limit the national security exceptions of Title III to "foreign" threats, comprised the entire Senate discussion.

The Senate's failure to define the nature of the legislative grant was duplicated during House debate. S. 917, drafted by the Senate Judiciary Committee and approved by the Senate, differed appreciably from the earlier House-approved bill, H.R. 5037. Accordingly, Rep. Emanuel Celler, the liberal chairman of the House Judiciary Committee, sought to refer the bill to conference. His attempt was stymied by House conservatives who exploited "law and order" and the effect on the public of the recent assassination of Robert Kennedy. The House then proceeded to vote on a resolution approving the Senate bill, debate on which was stringently limited by the Rules Committee. The hastiness of House consideration of the Senate bill and the time limits established for debate prevented opponents from rallying opposition or from raising probing questions to define the meaning of the bill's provisions.

At best, then, House analysis was perfunctory and superficial. Critics of Title III expressed their opposition in general terms, objecting as much to the constitutionality and repressive character of the authority to wire tap in criminal cases as to section 2511 (3)'s broad grant of Presidential authority in national security cases and its possible use for political surveillance.

House debate, as reported in the *Congressional Record*, did, however, reveal Congressional ignorance and misunderstanding of what exactly had been approved. This came out sharply in explanatory comments by Reps. William Randall (D., Mo.) and Howard Pollock (R., Alaska). (Their errors are the more striking since neither Representative exercised the option provided by the House rule permitting a member to revise within forty-eight hours any comments he has made during floor debate.) Thus, Randall affirmed that Title III limited abuses by requiring court approval before wire tapping. "Only in the case of national security," Randall continued, "can wire taps be made without a court order. And even these are invalid if application for such order *is not made within forty-eight hours* after such surveillance is undertaken." Pollock made a similar error. Law-enforcement officers, he said, had to secure

court approval except in certain "limited" cases where wire tapping was permitted for forty-eight hours "if it concerns national security or organized crime" which are of an "emergency" nature.

The lackadaisical nature of Congressional debate urgently raises important political and constitutional questions about Title III. Apart from the issue of whether wire tapping is an "unreasonable" search and seizure or a violation of First Amendments liberties is the question whether by this act the Congress unconstitutionally and irresponsibly delegated unwarranted authority to the executive. And, although the Supreme Court has for more than thirty years seen fit not to apply the *Schechter* decision, accepting instead broad delegations of power to the executive, the principle enunciated by Chief Justice Hughes in that case has bearing on the wire-tapping grant of the Omnibus Crime Control Act. Declaring the majority position of the Court, Hughes then affirmed:

> Extraordinary conditions may call for extraordinary remedies. . . . Extraordinary conditions do not create or enlarge constitutional power. The Constitution established a national government with powers deemed to be adequate, as they have proved to be in war and peace, but these powers of the national government are limited by constitutional grants. . . .
>
> The Congress is not permitted to abdicate or to transfer to others the essential legislative functions with which it is vested. We have repeatedly recognized the necessity of adapting legislation to complex situations involving a host of details with which the national legislature cannot deal directly. . . . But we said that the constant recognition of the necessity and validity of such provisions, and the wide range of administrative authority which has been developed by means of them, cannot be allowed to obscure the limitations of the authoriy to delegae, if our constitutional system is to be maintained. . . .
>
> . . . Section 3 [of the National Recovery Act of 1933] set up no standards, aside from the statement of the general aims. . . . In view of the scope of that broad declaration, and of the nature of the few restrictions that are imposed, the discretion of the President . . . is virtually unfettered.

This constitutional argument of legislative responsibility, it can thus be argued, equally and pointedly applies to executive authority in "national security" areas where, with the resort to wire tapping, an additional constitutional question is involved. The cold war has had a profound effect on American politics, especially as it has contributed to extending Presidential authority. As a result, traditional Congressional restrictions on executive powers in the military-foreign policy areas have been reduced, and the Court has avoided confronting executive authority in the "national security" area. At the least, this development has as one basis the President's prerogatives as Commander in Chief and his right to appoint ambassadors, formulate treaties, and shape foreign policy. But the same constitutional justification does not equally prevail in the internal security area, where executive authority is less clear and constitutional restrictions specifically limit administration investigative and prosecutive activities.

These considerations do raise two issues. First, whether Title III of the Omnibus Crime Control Act of 1968 is an exercise of legislative responsibility and, second, whether the title provides an unwarranted and unwise grant of authority, particularly in view of the process by which its provisions were reviewed and Congressional intent established. The other issue concerns the relationship between the President and the Department of Justice—which, if viewed historically, would require that the Congress be more judicious when ceding almost unlimited wire-tapping authority to the executive.

[From the Providence Sunday Journal, December 19, 1971]

KENNEDY, JUSTICE DEPARTMENT CLASH OVER WIRETAPS, "BUGS" EXTENT

WASHINGTON.—The Justice Department and Sen. Edward M. Kennedy, D., Mass., clashed yesterday over the number of wiretaps and "bugs" the government uses on grounds of national security.

Kennedy released a Justice Department letter which he said shows that the extent of such wiretapping and bugging is "substantially greater" than the government had led the public to believe.

The Justice Department responded, hitting at Kennedy's "erroneous and misleading allegations." The department statement said that there have never been more than 50 wiretaps in operation at any one time in the last three years, except for a few days in 1969 and in 1970.

The letter released by Kennedy was from assistant atty. gen. Robert C. Mardian and was the first government breakdown of wiretaps and bugs in the national security field.

The senator said the numbers are about two to three times higher than those cited in recent statement by President Nixon and Solicitor General Erwin N. Griswold and that the duration of the surveillances is three to nine times greater than those authorized by court order in criminal cases.

As chairman of the Senate subcommittee on administrative practice and procedure, Kennedy requested the electronic surveillance breakdown last February. Mardian's response came last March 1. Aides to Kennedy attributed the delay in releasing the letter to indecision on what to do with it.

SUBJECT OF CONTROVERSY

National security eavesdropping is a constant subject of controversy. The 1968 Omnibus Crime Act gave the government the authority to bug and tap in major criminal cases with court approval. The government has claimed the right to bug and tap without court order in national security matters. Whether such surveillance can be conducted legally on domestic groups as well as foreign nationals is a question currently being reviewed by the Supreme Court.

Wiretapping refers to interception of telephone conversations, while bugging is electronic eavesdropping on room conversations, usually with a microphone.

According to Mardian's letter the Justice Department operated 97 national security telephone surveillances and 16 national security microphone surveillances in 1970, or a total of 113 listening devices. This compares with 180 court-approved devices for the same year.

Mardian also disclosed that the maximum number of telephone taps in use at any given time during 1970 was 56; the maximum number of microphone bugs was six.

HOOVER NOT CONTRADICTED

The disclosures do not contradict the wiretap statistics annually cited by the Federal Bureau of Investigation director, J. Edgar Hoover. Hoover carefully couches his language to apply only to the number of surveillances on a given day, a reporting method that an American Civil Liberties Union study released a week ago characterizes as "highly misleading."

But Kennedy said the Mardian figures flatly contradict statements on the subject by Nixon and Griswold.

Last April, Kennedy said, President Nixon told the annual convention of the American Society of Newspaper Editors: "Now, in the two years that we have been in office—now get this number—the total number of taps for national security purposes by the FBI, and I know because I look, not at the information, but at the decisions that are made—the total number of taps is less, has been less, than 50 a year."

BRIEF IS CITED

Nixon compared this number with "only 300 taps" by the FBI through court orders over a two-year period, a transcript provided by Kennedy's office shows.

Justice department officials have said that only the FBI installs national security listening devices for the Justice Department.

Kennedy also cited a brief submitted by Griswold to the Supreme Court last September. It listed the number of national security telephone taps as 36 for 1970.

"The above figures are flatly contradicted by Mardian's March 1 letter to me, in which he reveals that a total of 97 warrantless national security telephone taps were operated in 1970—almost double the President's figure and almost triple the solicitor general's figure," Kennedy noted.

Neither Nixon nor Griswold referred to the number of microphone installations.

Kennedy Says Wiretap Gap Exists in United States

(By John Chadwick)

Washington.—Sen. Edward M. Kennedy, D., Mass., said Saturday that government wiretapping and bugging in national security cases is substantially greater than President Nixon and other administration officials have led the public to believe.

This type of electronic surveillance is conducted without court-issued warrants, as contrasted with a requirement that court authorization be obtained for government eavesdropping to combat domestic crime.

Kennely said figures obtained from the Justice Department bear out his recent contention that "there has been three to nine times as much federal listening going on as a result of warrantless electronic surveillance as there has been on devices operated under judicial authorization."

He made public an exchange of correspondence with Assistant Atty. Gen. Robert C. Mardian, in charge of the department's Internal Security Division.

ALLEGATIONS HIT

The Justice Department said Kennedy's allegations are "erroneous and misleading."

In a statement, the department said: "Any assertion that the total amount of federal electronic eavesdropping without court permission far exceeds the eavesdropping with judicial approval is false. The number of court-authorized devices in 1970 was 180, compared to 113 national security devices installed.

"Court-authorized taps, which are used solely for gathering evidence for use in criminal prosecutions, are limited to 30 days duration. There is no such limit for national security taps, which are solely for the purpose of intelligence gathering. To compare the two for the purpose of drawing inappropriate and preconceived conclusions doesn't serve the public interest."

The department said FBI records show there were never more than 50 wiretaps in operation at any one time in 1969, 1970 and 1971, except in two instances where authorizations overlapped for a matter of days. The microphone surveillance has never exceeded six at any one time in these years, it said.

Kennedy said figures supplied by Mardian contradict a statement by Nixon last April to the American Society of Newspaper Editors that the total number of taps for national-security purposes by the FBI has been fewer than 50 a year during his administration.

He said they contradict also a brief filed by the U.S. solicitor general in the Supreme Court saying that only 36 warrantless telephone surveilances were operated in 1970.

A letter he received from Mardian last March 1, Kennedy said, showed "that a total of 97 warrantless telephone taps were operated in 1970—almost double the President's figure, and almost triple the solicitor general's figure."

Kennedy said that in addition to the telephone taps, Mardian's letter showed there were 16 microphone installations used for bugging in 1970.

"Further," Kennedy said, "the repeated references by government officials to the limited number of warrantless devices ignore the far more significant question of the duration and total usage of these surveillances."

Mardian's March 1 letter listed 97 telephone surveillances without court order in 1970 and broke these down into four categories—those in operation less than a week, from a week to a month, from one to six months and more than six months.

Mardian requested that the number in each category be treated as confidential "since an examination of the breakdown might indicate a fixed number of permanent surveillances."

In compliance with Mardian's request, Kennedy didn't disclose the number in each category. But from the figures his staff prepared a table showing a range from a minimum of 8,100 to a maximum of 22,600 days in which listening devices were in operation by executive order in 1970.

Kennedy said that for the two-year period of 1969-1970, the staff calculations showed that "warrantless devices accounted for an average of 78 to 209 days of listening per device, as compared with a 13-day per device average for those devices installed under court order."

Thus, he said, the information obtained from Mardian "poses the frightening possibility that the conversations of untold thousands of citizens of this country are being monitored on secret devices which no judge has authorized and which may remain in operation for months and perhaps for years at a time."

[From the New York Times, December 19, 1971]

KENNEDY CHARGES JUSTICE DEPARTMENT HIDES EXTENT OF WIRETAPS

WASHINGTON.—Senator Edward M. Kennedy said today that the Justice Department ordered 207 electronic surveillances in 1969 and 1970 under executive authority, nearly equal to the 210 approved by the Federal courts.

In a letter to his colleagues on the Judiciary Committee, the Massachusetts Democrat provided the most comprehensive public disclosure yet of the so-called "warrantless" surveillances and charged that the figures contradicted official statements.

"Further," Mr. Kennedy said in his letter, "the repeated references by Government officials to the limited number of warrantless devices ignore the far more significant question of the duration and total usage of these surveillances."

Using figures provided by the Justice Department, the Senator declared that "there were from 3.4 to 9.6 times as many days of Federal listening on warrantless devices as there were on devices installed under judicial authorization."

Mr. Kennedy's assertion was based on Justice Department figures that showed that court-ordered devices in 1970 were in use a total of 2,363 days and executive-ordered devices a total og 6,100 to 22,600 days.

The specific duration of executive-ordered devices is not disclosed by the Justice Department. It supplies only a range of time—from one week to one month, for example.

The disclosures will probably intensify the controversy over the legality and extent of executive surveillances, but they may also serve to demonstrate the limits of the Administration's wiretapping practices, which some have called widespread.

Thus, if the figures are complete, it could be argued that they reflect a low level of wiretapping over the two-year period—one of every million citizens.

As for the duration of the surveillances used without court authority, Government officials have said that relatively longer periods reflect the routine use of devices over extended periods of time on such places as foreign embassies.

The distinction between the two kinds of electronic survillances derives from a Supreme Court decision in 1967 that declared that the use of wiretaps was unconstitutional in certain instances.

Subsequently, Federal legislation was approved to enable the Government to employ electronic surveillance under court authority in criminal investigations, but left it to the courts to decide to what extent the Government could use wiretaps and other such devices without court approval in cases involving internal security.

This question is pending before the Supreme Court.

CHART ILLUSTRATES USE

The wiretapping statistics were provided by Mr. Kennedy in his role as chairman of the Subcommittee on Administrative Practice and Procedure. He obtained them from Robert C. Mardian, Assistant Attorney General for Internal Security, in a letter dated last March 1.

A chart compiled by the subcommittee staff shows that there were 30 court-ordered devices used in 1969 and 180 in 1970. This compares with 94 executive-ordered devices in 1969 and 113 in 1970.

Mr. Mardian pointed out in his letter to Senator Kennedy that the maximum number of devices in operation at any one time was 64 for the year 1969 and 62 for 1970.

Mr. Kennedy said that the duration figures "pose the frightening possibility that the conversations of untold thousands of citizens of this country are being monitored on secret devices which no judge has authorized and which may remain in operation for months and perhaps years at a time."

He further charged that the figures "flatly contradict" public statements by the Administration.

He declared that a brief filed this year with the Supreme Court by Solicitor General Erwin N. Griswold said that only 36 warrantless telephone surveillances were operated in 1970. He also pointed to a statement on April 16, 1971, by President Nixon that "the total number of taps is less, has been less, than 50 a year."

A member of Mr. Kennedy's subcommittee staff said that Mr. Griswold's figure was apparently drawn from Congressional testimony by J. Edgar Hoover, director of the Federal Bureau of Investigation, in February 1970. The figure apparently refers to the number of devices in operation at the time.

Mr. Nixon's figure is also believed to refer to the number of devices in use at the time of his statement.

Mr. Kennedy said the letter from Mr. Mardian suggested "an absence of well-defined procedures" to promote compliance with the statutes under which executive-ordered surveillance is conducted.

Thus, he said, he found it "shocking" that the department did not maintain a breakdown of executive-ordered surveillances under the five categories authorized by law.

[From the Baltimore Sun, December 19, 1971]

KENNEDY CASTS DOUBTS ON NIXON'S WIRETAP FIGURES

WASHINGTON—Senator Edward M. Kennedy (D., Mass.) said yesterday that government wiretapping and bugging in national-security cases is substantially greater than President Nixon and other administration officials have led the public to believe.

This type of electronic surveillance is conducted without court-issued warrants, as contrasted with a requirement that court authorization be obtained for government eavesdropping to combat domestic crime.

Mr. Kennedy said figures obtained from the Justice Department bear out his recent contention that "there has been three to nine times as much federal listening going on as a result of warrantless electronic surveillance as there has been on devices operated under judicial authorization."

He made public an exchange of correspondence with Robert C. Mardian, an assistant attorney general, in charge of the department's Internal Security Division.

The Justice Department said Mr. Kennedy's allegations were "erroneous and misleading."

In a statement, the department said: "Any assertion that the total amount of federal electronic eavesdropping without court permission far exceeds the eavesdropping with judicial approval is false. The number of court-authorized devices in 1970 was 180, compared to 113 national-security devices installed.

"Court-authorized taps, which are used solely for gathering evidence for use in criminal prosecutions, are limited to 30 days duratoin. There is no such limit for national-security taps, which are solely for the purpose of intelligence gathering. To compare the two for the purpose of drawing inappropriate and preconceived conclusions does not serve the public interest."

The department said FBI records show that there were never more than 50 wiretaps in operation at any one time in 1969, 1970 and 1971 except in two instances where authorizations overlapped for a matter of days. The microphone surveillance has never exceeded six at any one time in these years, it said.

Mr. Kennedy said figures supplied by Mr. Mardian contradict a statement by Mr. Nixon last April to the American Society of Newspaper Editors that the total number of taps for national-security purposes by the FBI has been fewer than 50 a year during his administration.

He said the figures contradict also a brief filed by the U.S. solicitor general in the Supreme Court saying that only 36 warrantless telephone surveillances were operated in 1970.

A letter he received from Mr. Mardian last March 1, Mr. Kennedy said, showed "that a total of 97 warrantless telephones taps were operated in 1970—almost double the President's figure, and almost triple the solicitor general's figure."

Mr. Kennedy said that, in addition to the telephone taps, Mr. Mardian's letter showed there were 16 microphone installations used for bugging in 1970.

"Further," Mr. Kennedy said, "the repeated references by government officials to the limited number of warrantless devices ignore the far more significant question of the duration and total usage of these surveillances."

Mr. Mardian's March 1 letter listed 97 telephone surveillances without court order in 1970 and broke these down into four categories—those in operation less than a week, from a week to a month, from one to six months and more than six months.

Mr. Mardian requested that the number in each category be treated as confidential "since an examination of the breakdown might indicate a fixed number of permanent surveillances."

In compliance with Mr. Mardian's request, Mr. Kennedy did not disclose the number in each category. But from the figures his staff prepared a table show- a range from a minimum of 8,100 to a maximum of 22,600 days in which listening devices were in operation by executive order in 1970.

Mr. Kennedy said that over the two-year period of 1969 through 1970, the staff calculations showed that "warrantless devices accounted for an average of of 78 to 209 days of listening per device, as compared with a 13-day per device average for those devices installed under court order."

Thus, he said, the information obtained from Mr. Mardian "poses the frightening possibility that the conversations of untold thousands of citizens of this country are being monitored on secret devices which no judge has authorized and which may remain in operation for months and perhaps for years at a time."

Staff aides of Mr. Kennedy, chairman of a Senate Judiciary Committee's subcommittee on administrative practices and procedures, said, in response to newsmen's questions, that some of the national security taps, as in the case possibly of foreign embassies, might be virtually permanent installations.

The said also, as did Mr. Kennedy, that they did not know how many of them involved foreign-intelligence operations as distinguished from domestic disidents.

Mr. Kennedy, in a letter to his colleagues on the subcommittee, said that if 95 per cent of installations were solely for obtaining foreign-intelligence information from aliens and only 5 per cent for surveillance of domestic dissidents regarded by the attorney general as a threat to the national security, the meaning would be quite different than if the figures were reversed.

[From the Boston Globe, December 19, 1971]

WIRETAP FIGURES DISPUTED

(By S. J. Micciche)

WASHINGTON.—President Nixon was only half right in telling the nation that the number of internal security wiretaps installed by his Administration without a court order is less than 50 a year, US Sen. Edward M. Kennedy reported.

That figure, said Kennedy, is "flatly contradicted" by none other than Asst. Atty. Gen. Robert C. Mardian, in charge of the Justice Department's Internal Security Division.

Moreover, the Massachusetts senator said that his correspondence with Mardian over several months is at even greater odds with the figure of 36 wiretaps in operation in 1970 cited by US Solicitor General Erwin N. Griswold in the government's brief with the US Supreme Court on a pending constitutional test of electronic surveillance.

Mardian informed Kennedy that during 1970 Atty. Gen. John N. Mitchell, acting for the President, had installed 97 telephone taps and 16 microphonic taps without court approval in internal security areas.

Kennedy, as chairman of the Senate Subcommittee on Administrative Practices and Procedures, had demanded from the Justice Department a breakdown in the number of taps, their days in use, and their category in terms of foreign intelligence information or the surveillance of domestic dissidence.

In more than just arithmetic discrepancy, Kennedy said the response by Mardian indicated a seeming inconsistence with State Departmental policy.

In refusing Kennedy a breakdown in the number of wiretaps for foreign or domestic security reasons, Mardian first reported that "no such categorization exists."

When later pressed by Kennedy, Mardian responded that the Justice Department "has never attempted such a categorization."

Mardian's replies in this regard, said Kennedy, are "absolutely shocking."

In his report to other members of the Senate subcommittee, Kennedy noted that in government briefs with the Supreme Court the Justice Department has maintained that the discretionary wiretaps by Mitchell were installed within the "statutory categories" permitted under the Safe Streets Act of 1968.

From Mardian's reply, Kennedy said, the "fairly explicit admission . . . is that there really are no procedures to assure adherence in advance to the statutory standards."

Instead, Kennedy said it is the "lone judgment of the Attorney General based on each separate submission to him by the (FBI) investigators who wish to do the surveilling" that determines the wire-tap and it is done "without specific focus on the statutory criteria."

Kennedy indicated to his subcommittee, colleagues that he might launch hearings into the Justice Department's use of wiretaps to determine the extent of its compliance with the congressional mandate.

Under the Federal statute, court orders are not required in the area of internal security.

Of the five categories "of danger to the nation" listed by Congress as the standard to permit wiretaps without court authorization, three concern foreign intelligence and two are directed toward domestic subversion.

From his correspondence with Mardian, Kennedy has concluded that the extent of Federal "bugging" without court authority "is substantially greater than the Executive Branch has led the public to believe."

[From the Evening Star, December 19, 1971]

How Much Eavesdropping?

(By Lyle Denniston)

The Nixon administration last year used twice as many secret eavesdropping devices without court approval as the number previously disclosed, Sen. Edward M. Kennedy, D-Mass., charged yesterday.

In reply, the Justice Department accused Kennedy of making "erroneous and misleading" conclusions, and insisted that the use of wirtaps and hidden microphones has declined sharply.

The dispute broke out as Kennedy made public a letter he had written to members of a Senate Judiciary subcommittee which he heads, saying national security eavesdropping is "apparently far more pervasive than any of us had ever realized."

The department, commenting on the letter, said the senator was "drawing inappropriate and preconceived conclusions" which it said "do not serve the public interest."

DATA CITED

Citing data he had received from the Justice Department, Kennedy said 97 telephones wiretaps and 16 hidden microphones were installed without court approval in national security cases in 1970.

This "flatly contradicted" a public statement by President Nixon last April that the number was "less than 50 a year," the senator said.

He also said the data was far different than that Solicitor General Erwin M. Griswold had given the Supreme Court in September. Griswold said there were only 36 wiretaps used in 1970, and he made no mention of hidden microphones.

The Justice Department, in its reply to Kennedy, said its policy had been to reduce both the number of listening devices in place at any one time and the total number in use throughout a full year.

The official statement emphasized the number of devices in use at any given time, rather than the year total.

50 WIRETAPS

In 1969, 1970, and 1971, the statement said, no more than 50 wiretaps were operating at any time except twice, once in 1969 and once in 1970, where there were more than 50 over a period of days.

In the same three-year period, the department added, the number of hidden microphones in use was never more than six at a time.

Turning to the annual figures, the department conceded the total of 113 devices—the 97 telephone wiretaps and 16 hidden microphones—about which it had told Kennedy.

It added that the total used between January and Oct. 15 of this year was 85-79 wiretapes and six microphones.

During that period, it said, there were never more than 43 wiretaps being used at a time.

As of Friday, the statement said, there were 32 wiretaps and four microphones in operation in national security cases.

RULING EXPECTED

The dispute between Kennedy and the department and the figures which each discussed are confined to national security eavesdropping because that is the only kind which the Nixon administration says it has power to conduct without court orders.

The Supreme Court is expected to rule next year on the administration's claim that the only approval needed is that of the attorney general acting on behalf of the president.

This authority, Atty. Gen. John N. Mitchell has said, applies to secret monitoring of "domestic subversives" who threaten the government as well as to foreign agents who threaten espionage.

Kennedy's letter was based primarily from the Justice Department March 1 in reply to inquiries about the scope of eavesdropping without court approval.

EXPLANATION AWAITED

The senator's staff said he was releasing the data now rather than earlier because he had hoped to get a fuller explanation from the department about the details of national security surveillance.

Complaining in his letter about repeated comments by government officials about the limited number of national security surveillances, Kennedy said that the data given to him "poses the frightening possibility that the conversations of untold thousands of citizens of this country are being monitored on secret devices which no judge has authorized and which may remain in operation for months and perhaps years at a time."

The data released by Kennedy showed there were 94 national security listening devices used in 1969, with 81 of them wiretaps and 13 hidden microphones.

Kennedy's staff analyzed additional data which the department had supplied but which was not released last night, and drew the conclusion that this showed the actual volume of eavesdropping done without court order "far exceeds" that done with court approval in nonsecurity cases.

SECRET DATA

This conclusion was based on still secret data about the duration which national security devices are left in operation.

For 1970, the staff data showed, national security devices were used between 3.4 and 9.6 times as long as nonsecurity devices were used.

Kennedy's letter cited this data and said it, too, contradicts the impression that national security surveillance is a strictly controlled activity of the government.

The Justice Department reply to Kennedy described as false the suggestion that there was more surveillance without court approval than there was with it.

It said that court-approved devices are limited to 30-day periods, while there are no limits on national security devices. The national security devices, the department said, are not used to gather criminal evidence as the court-approved devices are, but instead are used only to gather intelligence data.

The department noted that there were 180 court-authorized devices used in 1970, compared with 113 national security devices.

[From the Washington Post, December 19, 1971]

Wiretap Extent Disputed

(By Ronald Kessler)

Sen. Edward M. Kennedy has released a Justice Department letter which he says shows that the extent of government wiretapping and bugging in national security cases is "substantially greater" than the government has led the public to believe.

The letter, from Assistant Attorney General Robert C. Mardian, is the first government breakdown of taps and bugs in the national security field.

Calling Kennedy's statement "erroneous and misleading," the Justice Department late yesterday cited figures to show that the amount of government eavesdropping has decreased in the past 10 years.

Kennedy, however, had made no claim that the amount of tapping and bugging had gone up or down.

The Massachusetts Democrat charged that the number of bugs and taps listed in Mardian's letter conflicted with statements of administration officials.

Specifically, he said that the Mardian figures are about two to three times higher than the number of taps cited in recent statements by President Nixon and Solicitor General Erwin N. Griswold. Kennedy also said that the duration of the surveillances is three to nine times greater than the duration of those authorized by court order in criminal cases.

As chairman of the Senate Subcommiittee on Administrative Practice and Procedure, Kennedy requested the electronic surveillance breakdown last February. Mardian's response came March 1. Aides to Kennedy attributed the delay in releasing the letter to indecision on what to do with it.

National security eavesdropping is a constant object of controversy. The 1968 Omnibus Crime Act gave the government the authority to bug and tap in major criminal cases with court approval; the government has claimed the right to bug and tap without court order in national security matters. Whether such surveillance can be conducted legally on domestic groups as well as foreign nationals is a question currently being reviewed by the Supreme Court.

Wiretapping refers to interception of telephone conversations, while bugging is electronic eavesdropping on room conversations, usually with a microphone.

According to Mardian's letter, the Justice Department operated 97 national security telephone surveillances and 16 national security microphone surveillances in 1970, or a total of 113 listening devices. This compares with 180 court-approved devices for the same year.

Mardian also revealed that the maximum number of telephone taps in use at any given time during 1970 was 56; the maximum number of microphone bugs was six.

The disclosures do not contradict the wiretap statistics annually cited by Federal Bureau of Investigation Director J. Edgar Hoover. Hoover carefully couches his language to apply only to the number of surveillances on a given day.

But Kennedy said the Mardian figures "flatly" contradict statements on the subject by President Nixon and Solicitor General Griswold.

Last April, Kennedy wrote, President Nixon told the annual convention of the American Society of Newspaper Editors:

"Now, in the two years that we have been in office—now get this number—the total number of taps for national security purposes by the FBI, and I know because I look not at the information but at the decisions that are made—the total number of taps is less, has been less, than 50 a year."

Mr. Nixon compared this number with "only 300 taps" by the FBI through court orders over a two-year period, a transcript provided by Kennedy's office shows.

Justice Department officials have said that only the FBI installs national security listening devices for the Justice Department.

Kennedy also cited a brief submitted by Griswold to the Supreme Court last September. It listed the number of national security telephone taps as 36 for 1970.

The Justice Department countered yesterday that Kennedy's assertion that "'the total amount of federal electronic eavesdropping without court permission far exceeds the eavesdropping with judicial approval" is false. The number of court-authorized devices, the department noted, was 180 in 1970, compared with 113 national security devices.

Justice also pointed out that court-authorized eavesdropping is limited to 30 days' duration, while there is no limit on national security installations.

"To compare the two for the purpose of drawing inappropriate and preconceived conclusions does not serve the public interest," Justice said.

[From the New York Times, December 19, 1971]

A Gross Invasion

(By Tom Wicker)

Prof. Herman Schwartz of the law faculty at the State University of New York in Buffalo is a busy man. He has been working nonstop this fall to protect the legal rights and in some cases the physical well-being of prisoners who were in revolt at Attica last September. He is also managing several suits by reporters for better access to prisons and prisoners, and now he has compiled the most complete figures available on the extent, cost and results of electronic surveillance in America. They are shocking.

These figures tend to support what opponents of tapping and bugging have long maintained—that eavesdropping costs too much money and represents too great an invasion of individual rights to be justified by the meager results obtained. And Mr. Schwartz is at pains to point out that even those results had virtually nothing to do with the kind of violence usually associated with "law and order."

Now Senator Edward M. Kennedy has release figures he obtained from the Justice Department showing that so-called "national security" eavesdropping without court orders is engaged in far more broadly than the Justice Department or the FBI had previously admitted.

The net effect of the Schwartz and Kennedy figures is to expose the shell game the Nixon Administration and other hard-nose types have been playing with the issue of wiretapping and bugging. By citing these procedures loudly in their law-and-order rhetoric, they leave the impression that eavesdropping helps in cracking down on those who mug and rape and murder; by careful selection of their own figures, they make eavesdropping seem less excessive and more effective than it is; and by citing only court-ordered eavesdrops, they canceal the extent to which they are tapping, without court orders, those they regard as subversives.

For instance, Mr. Schwartz points out that both J. Edgar Hoover and Attorney General John Mitchell said last spring that there were fewer than forty national security eavesdropping installations, a figure that compares well with the number of court-ordered surveillances in 1970, which was 180.

But the fewer-than-forty figures was for installations *at any one time*—not for a whole year. Mr. Schwartz checked and found out that on several days chosen at random there also were far fewer than forty court-ordered surveillances in nonsecurity cases, Senator Kennedy's figures showed 94 national-security surveillances in 1969 and 113 in 1970; but the Attorney General previously had published figures claiming, on the misleading at-any-one-time basis, that there had been a maximum of 49 national-security surveillances in 1969 and only 36 in 1970, so that such operations were in fact declining.

Again, when the public is told that there were only 302 court-ordered electronic surveillances in 1969, that does not sound like so many—particularly since only 271 operations actually were installed (these figures are for state and Federal eavesdropping). But it becomes quite a different picture when that means, as Mr. Schwartz shows that 31,436 people were overheard in 173,711 conversations. And when the smaller totals for 1968 and the greater totals for 1970 are added, it can be seen that in those three years alone, 61,400 people and 622,292 conversations were overhead *not counting all those eavesdropped upon without a court order and for so-called "national security" purposes.* And the trend is up.

What did all this have to do with crimes of violence? In 1970, Federal officers eavesdropped in not a single murder or kidnapping case, but rather on 119 gambling cases, 40 narcotics cases, 16 credit extortion cases, and a few miscellaneous cases. Most state eavesdropping also is aimed at gambling.

Besides, all that listening-in produced in 1970 only 613 arrests and 48 convictions from among the 10,260 people and 147,780 conversations overheard.

The state snoops did a little better; they got 103 convictions, but then they listened in on half again as many conversations. Federal eavesdropping produced *no* convictions for anything other than gambling.

None of this comes cheap, not at those conviction rates. In 1970, Federal and state surveillance was reported to have cost $3 million and the 1971 cost is projected at closer to $5-million, but these are gross under-estimates. Most importantly, they do not include the cost of "national security" tapping without court orders.

Nor do the official cost reports take any account at all of the vast amount of time lawyers, judges and investigators take to prepare applications, keep records and handle court challenges. Mr. Schwartz believes the actual cost of eavesdropping may be "many times the 1970 figure of $3-million." The lion's share of all that money is being spent to try to control gambling—which is not the kind of crime most of us thought Mr. Nixon had in mind during his 1968 campaign.

It all adds up to what Herman Schwartz calls "gross and widespread invasions of privacy" in order to get "a handful of convictions of gamblers, pushers and the like." Surely, he suggests, "we have less pernicious ways to spend our scarce dollars."

Wiretaps and National Security

(Alan M. Dershowitz)

(Alan M. Dershowitz, professor of law at Harvard, is currently at the Center for Advanced Study in the Behavioral Sciences at Stanford)

During its current term, the Supreme Court will be hearing argument on whether warrantless "national-security" wiretaps are constitutional. The phrase "national security" conjures up the image of spies, sabotage, and invasion, but a considerable number of such taps are conducted against domestic organizations or individuals who are suspected of activities deemed contrary to the national interest. It was recently learned, for example, that such persons as Martin Luther King and Elijah Muhammad and such organizations as the Jewish Defense League and the Black Panther party have been the subject of extended national-security taps. These taps are authorized exclusively by the prosecutorial arm of the government—by the attorney general—without the need for a judicial warrant based on probable cause. How many national-security taps and "bugs"[1] are currently in operation, and against what sorts of persons, is a well-guarded secret, but bits of information that are slowly emerging raise some disturbing questions.

The case presenting the issue of the constitutionality of warrantless national-security taps involves "Pun" Plamondon, an alleged "White Panther standing trial for conspiracy to blow up a CIA office in Ann Arbor, Michigan. Plamondon's lawyer, William Kunstler, filed a pre-trial motion asking the government to disclose whether any of the defendant's conversations had been monitored. Motions of this kind are made rather routinely these days in so-called political cases, and—not infrequently—they strike paydirt, as Kunstler's motion did. It elicited an affidavit from the attorney general himself, acknowledging that "Plamondon has participated in conversations which were overheard by government agents," and that no warrant had been obtained. But Mitchell vigorously asserted that the tap—which was on some unnamed person's phone, not on Plamondon's—was legal, since it was "employed to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the government."

---

[1] A "bug" is a monitoring device concealed anywhere and capable of picking up conversations as well as other sounds; a wiretap picks up only phone conversations. Some confusion has resulted from the fact that "bugs" are sometimes installed in the mechanism of a telephone. The government is fond of citing statistics purporting to demonstrate that the number of "national-security surveillances"—a phrase that includes both bugs and taps—has "significantly declined" over the past few years. These statistics are fallacious for two obvious reasons: 1) they include figures only on the number of warrantless taps, not bugs; and 2) they show a decline around the time the Supreme Court implicitly authorized the use of taps with a warrant. (Prior to that decision, all taps involving national security were warrantless, and were therefore included in the government statistics; now warrants are secured for some of these taps, and only the warrantless ones are listed by the government.)

The lower court disagreed. It described the "sweep of the assertion of the Presidential power" to tap without a warrant as "both eloquent and breathtaking," but it declined to "suspend an important principle of the Constitution." It held that "in dealing with the threat of domestic subversion," the warrant requirement of the Fourth Amendment could not be dispensed with. (The lower court did not decide whether a warrantless tap could be authorized to protect the country from "attack, espionage or sabotage by foes or agents of a *foreign power*," since the government had conceded that the Plamondon tap was not installed for any such "foreign intelligence" purpose.)[2] The court ordered the government to disclose to Plamondon the transcripts of each of his monitored conversations. If this ruling is upheld, Plamondon could be tried and convicted only if the government can prove that neither the indictment nor any of the trial evidence emanated from the tainted tap.

The issue thus presented for the Supreme Court to resolve is a fundamental one, going to the heart of the "separation of powers" on which our government is based. For the executive branch is asserting the power to dispense with an important judicial "check" on its action, namely the requirement that a judicial officer determine whether there is probable cause on which to issue a warrant. It is somewhat surprising that the Supreme Court has never decided—or even intimated how it would decide—whether national-security wiretaps constitute an exception to the warrant requirement, especially since the practice of warrant-less national-security taps is now more than thirty years old.

It was on May 21, 1940 that President Franklin Roosevelt sent to his attorney general the confidential memorandum that is regarded as the baptismal certificate of the national-security wiretap (though, significantly, the term "national security" was not used).[3] Roosevelt began by expressing his agreement with an early Supreme Court decision that "under ordinary and normal circumstances wiretapping by Government agents should not be carried on for the excellent reason that it is almost bound to lead to abuse of civil rights." But these were not ordinary and normal times: America was preparing to enter the war; German and Japanese spy rings were operating on both coasts; and "certain other nations" had been engaged "in preparation for sabotage." Concluding that the Supreme Court had never intended its prohibition on wiretapping to extend "to gave matters involving the defense of the nation," Roosevelt informed the FBI that they were "at liberty to secure information by listening devices direct[ed] to the conversations . . . of persons suspected of subversive activities against the government . . . , including suspected spies."[4] The President cautioned, however, that these investigations must be limited "to a minimum" and "insofar as possible to aliens."

But governments grow comfortable with special war powers, even when peace returns. And so, after the cessation of hostilities, Attorney General Tom Clark convinced President Truman that "the present troubled period in international affairs, accompanied as it is by an increase in subversive activity here at home," required a continuation of the "investigative measures" authorized by Roosevelt. Nor was Clark content merely with retaining the status quo. Warning that "the country is threatened by a very substantial increase in crime"—an exaggeration typically made by attorneys general requesting additional powers or appropriations—he "reluctantly" requested the President to approve the power to tap "in cases vitally affecting the domestic security" (for that high-

---

[2] The American Bar Association Project on Minimum Standards for Criminal Justice "considered and rejected [a proposal] which would have recognized a . . . power in the President not subject to prior judicial review to deal with purely domestic subversive groups." Instead, it recognized a power limited to "foreign intelligence activities." Thus, it is precisely the power rejected by the ABA committee—certainly no radical organization—that the government is asserting in the Plamondon case. In its brief before the Supreme Court, the government argues that no real distinction can be drawn between foreign and domestic subversion (though in prior cases it had argued in favor of such a distinction). Moreover, if no distinction can be drawn between foreign and domestic subversion, it would seem to follow that warrants should be required in both cases. Finally, a real distinction can be drawn between foreign-intelligence gathering and domestic subversion.

[3] The baptismal rather than the birth certificate, because it is acknowledged that J. Edgar Hoover was widely engaged in such wiretaps well before obtaining the President's formal authority to do so.

[4] Since the McCarthy era the word "subversive" has taken on an extremely broad meaning. At the time Roosevelt used it in his 1940 memorandum, it still retained its somewhat narrower (though still imprecise) dictionary meaning: "intended to bring about the overthrow of the government by unlawful means."

sounding phrase, read "organized crime") or "where human life is in jeopardy" (for that, read "murder, kidnapping, robbery, arson, burglary, and the sale of narcotics"). With Truman's quick concurrence, the narrow exception virtually became the rule. It was President Johnson who—at the urging of another Clark (this one more sensitive to civil liberties)[5]—again narrowed exception. In doing so, he introduced the current phrase "national security" which falls somewhere between Roosevelt's national "defense" and Truman's "domestic security."

It is not entirely clear why the government needs a national-security exception to the ordinary rules now governing wiretaps. When the exception was first created, there was an absolute prohibition against all wiretapping by federal officials—*with or without a warrant.* (The rule was not technically framed in terms of a prohibition on tapping, but rather in terms of a prohibition on all use of such evidence—and its fruits—in federal criminal prosecutions.) Thus, if national-security wiretaps were to be conducted at all, they would have to be authorized under an exception to the ordinary rules. In 1967, however, the Supreme Court said that wiretaps could be conducted—where any kind of criminal conduct was suspected—provided that the government secured a warrant based on probable cause and narrowly limited in time and scope. Under that decision, the FBI may lawfully conduct wiretaps in national-security cases if they secure a warrant. Unwilling to comply with this requirement, the federal government claims that national-security taps are still an exception to the ordinary rules, even though the ordinary rules which gave rise to the national-security exception have now been dramatically changed.

The government, arguing in support of this position before the lower courts, invoked "the inherent power of the President to safeguard the security of the nation"—the "historical power of the sovereign to preserve itself." The government was saying, in effect, that there is no separation of powers—no checks or balances on the executive by the other branches—when the President decides that the security of the nation is involved. The President must be trusted to exercise his powers in a constitutional manner, since "the occupant of that office, like the members of this Court, takes a solemn oath to protect and defend the Constitution," and this "carries with it the weightiest presumption that those powers will not be abused." (The attorney general—to whom the President has delegated all authority in these matters—also takes such an oath; but it is not without relevance that the attorney general is the country's top prosecutor; nor is it immaterial that two of the holders of this office during the past ten years have also been Presidential campaign managers, intensely involved in partisan politics.) If by some chance these powers were to be abused by the President or his deputies, the argument continues, then the "final significant restraint" lies not with the courts, but with the "electorate" which "can reflect its dissatisfaction with the exercise of the power."

This argument—which entirely neglects the counter-majoritarian purpose of the Bill of Rights and the anti-centralist thrust of the Constitution itself—has been rejected by the Supreme Court over and over again. The classic response was formulated in a case growing out of Lincoln's attempt to limit the judicial power during the Civil War:

> This nation, as experience has proved . . . , has no right to expect that it will always have wise and humane rulers, sincerely attached to the Constitution. Wicked men, ambitious of power, with hatred of liberty and contempt of law, may fill the place once occupied by Washington and Lincoln. . . . If our fathers had failed to provide for just such a contingency, they would have been false to the trust reposed in them. They knew—the history of the world had told them—that unlimited power, wherever lodged at such a time, was especially hazardous to freemen.

More recently, the Supreme Court rejected a similar assertion of executive power in the Pentagon Papers case, and it was probably this rejection that led the government to play down the "inherent power" argument in its wiretap brief recently filed in the Supreme Court. Instead, the government is now claiming that warrantless national-security taps were authorized by Congress in the Omnibus Crime Control and Safe Streets Act of 1968.

---

[5] In fairness to Justice Clark, it should be noted that subsequently he became quite critical of wiretapping.

That act actually provides three separate national-security exceptions to its otherwise absolute requirement of a warrant before any tap. The first authorizes a 48-hour tap if "an emergency situation exists" with respect to "conspiratorial activities threatening the national-security interests," provided that a warrant is immediately sought at the expiration of that period. The government did not act pursuant to that emergency exception in the Plamondon case. Nor is it relying on the second exception, which is limited to the prevention of attack by a foreign enemy or the gathering of foreign intelligence information. The "exception" which is being relied on by the government provides as follows: "Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government." That provision, however, begs the critical question: "What precisely is 'the constitutional power of the President' in dealing with domestic threats to the structure and existence of the government?" As the lower court observed, the 1968 act was "clearly designed to place Congress in a completely neutral position in the very controversy with which this case is concerned." Moreover, even if Congress had explicitly exempted domestic national-security wiretaps from the warrant requirement of the Fourth Amendment, the constitutionality of that exemption would still have to be decided by the Supreme Court.[6]

In passing on that difficult constitutional question, the Supreme Court might well ponder why the government is so vigorously asserting its right to dispense with warrants in national-security cases. Is it interested merely in preserving its convictions in the few pending cases that might be reversed if warrantless taps, conducted years ago, were held unconstitutional? Or does it have a real—and legitimate—need to tap phones without judicial intervention—need to tap phones without judicial intervention in this category of cases? There is little doubt that it could secure a warrant in any case in which there were a plausible—even a weak—claim that the national security required a tap. After all, the government may seek its warrant from the magistrate or judge of its choice. In the unlikely event that it were to fail on the first (or even the second) attempt, it could continue until it succeeded.[7]

The government explains its unwillingness to comply with the warrant requirement by suggesting that compliance would pose problems of security, presumably because an indiscreet or corruptible judge or court employee might betray the tap or disclose the identity of a secret informant whose information was used in the warrant application. But the government's wide discretion in selecting the judge before whom it will make the application diminishes the force of this argument. Surely there are some judges whose patriotism and discretion are beyond question in the view of the government. In an extremely delicate case, for example, the government could present its application to the Chief Justice without even the clerk being made privy to its contents. Moreover, under existing law, the government need not disclose the name of its informant—even to the judge in secret—in order to secure a warrant. Finally, the government concedes that in the event of a prosecution against anyone whose conversation was overheard, it must disclose the entire record of the tap to a judge in a secret proceeding (as it did in the Plamondon case). Now, if the government is willing to trust the discretion of a judge (selected at random) not to disclose the contents of a tap after it has occurred, why is it not willing to trust the discretion of a judge (chosen by the government) not to reveal the existence of a tap before it has occurred? The "indiscreet judge" ar-

---

[6] The Fourth Amendment does not unambiguously require a warrant for all searches. It provides for the right to be secure "against unreasonable searches," and it also specifies that "no warrant shall issue, but upon probable cause. . . ." The court, however, has interpreted the amendment to require a warrant for all searches, except in a narrow class of emergencies—for example, where there is imminent danger that the evidence will be destroyed. In such cases, the search must be justified, after the fact, as "reasonable" if its fruits are to be employed. But the government has taken the position that the usual standard of reasonableness is inapplicable to a national-security wiretap, even in an after-the-fact judicial evaluation. It argues that "great deference must be given to the attorney general's judgment" and that the range of review is "extremely limited."

[7] Of the 217 wiretap-warrant applications during the last two years, only one was denied.

gument, though vigorously pressed by the government, is obviously a make-weight.

There is a weightier argument against requiring a warrant in national-security cases, but the government has been reluctant to articulate it. A warrant, after all, must be based on probable cause that a crime has been, is being, or is about to be committed. The government would like to be free, however, to conduct certain wiretaps even when probable cause is lacking. For example, the Soviet ambassador engages in no crime when he discusses his country's negotiating position on the Mideast or the SALT talks, but our government would like to—and surely will try to—monitor such conversations (as the Soviet government just as surely tries to monitor similar conversations by our diplomats). If a warrant, based on ordinary probable cause, were required, the monitoring of this kind of conversation would become legally impossible.[8]

But this argument, which has considerable force in the context of foreign-intelligence wiretapping, is wholly inapplicable to the kind of tapping at issue in the case now before the Supreme Court. For the tap in the Plamondon case was not installed for purposes of gathering foreign intelligence; it was installed, in the words of the government, "to protect the national security against the threat posed by individuals and groups within the United States." Put most generously to the government, this means that the tap was directed against American citizens and organizations suspected of engaging in and planning bombings, riots, and other violent activities. All such activities are, of course, illegal, and anyone who is planning them—or even talking about planning them—is, under present government thinking, guilty of conspiracy (witness the Berrigan indictment). Surely, in any such case there would be little difficulty in obtaining a warrant. Yet the government insists that it must—and that it will—continue to tap phones without securing the judicial approval that it could so readily get in any plausible case.

If it is true that warrants in national-security cases would be so easy to obtain, then another question—really the converse of the question previously posed—is suggested: Why do civil libertarians press so hard for what appears to be the hollow protection of a warrant secured from a government-selected magistrate? Or to put it another way, why is the warrant issue viewed as so crucial by both sides?

To understand why civil libertarians feel the way they do about warrants in national-security cases requires a bit of background on the way they view wiretaps in general. To begin with, a great many civil libertarians oppose all wiretapping, even when authorized by warrant. They single out that technique of law enforcement because of its tendency to be indiscriminately over-inclusive. As Ramsey Clark has put it: "No technique of law enforcement casts a wider net than electronic surveillance. Blind, it catches everything in the sea of sound but cannot discriminate between fish and fowl." Of course, no technique of law enforcement casts a perfectly narrow net. We do, after all, convict some innocent people; we shoot some fleeing "felons" who turn out to be guiltless bystanders; we preventively detain some defendants who are ultimately acquitted. But we do insist, as we should, that these deprivations be imposed mostly on people who are guilty, and only rarel yon those who are innocent.

Wiretapping is different. It is a deprivation that falls mostly on the innocent. The ratio of "innocent" monitored conversations to "guilty" monitored conversations is extremely high, especially in national-security cases. This is so for a number of reasons. National-security taps are often installed on the phones of persons who are conceded to be innocent of any wrongdoing. And even taps installed on the phones of persons who are themselves guilty succeed in picking up the conversations of many innocent callers and recipients of calls. Finally, most of the monitored conversations, even between two guilty persons, involve matters unrelated to any wrongdoing. Moreover, because wiretapping is a clandestine "deprivation," its precise effects are difficult to assess. The behavior of some persons whose conversations are not, in fact, being moni-

[8] A warrant requirement would not necessarily prevent the continuation of all warrantless taps. It would merely prevent prosecution in the small number of cases where a defendant's conversations were overheard. Recently, however, an affirmative suit was filed on behalf of the Jewish Defense League seeking monetary damages for the warrantless tapping of their telephones.

tored is significantly affected by the *fear* that their phones are tapped (witness the "debugging" operations recently conducted by various Senators and Congressmen), while others, whose phones are being tapped, but who do not—and never will—know that their conversations were monitored, are entirely unaffected. Yet despite the pervasiveness of the wiretap, and its obvious chilling effect, the government blandly asserts in its brief that "[t]he overhearing of a telephone conversation involves a lesser invasion of privacy than a physical search of a man's home or his person." (This assertion sharply raises the question of whether an administration that values the privacy of conversation and thought less than the privacy of property is the appropriate authority to decide, without any judicial check, that a phone must be tapped for national-security purposes.)

Making national-security taps conditional on a warrant, some civil libertarians argue, would reduce the ratio of innocent to guilty conversations overheard because warrants must be narrowly circumscribed, limited in time and scope, and related to criminal conduct. While recognizing that most magistrates issue wiretap warrants as if they were presents at Christmastime, the civil libertarians contend that there might be some reluctance to issue them in instances where it was plain that the primary motivation was political and that the national-security concern was a pretext. For it is widely assumed by civil libertarians today that a considerable number of domestic national-security wiretaps are conducted primarily for reasons unrelated to genuine national-security concerns. They are thought to be directed against political dissidents—both inside and outside the government—and general troublemakers who could be adequately, and lawfully, dealt with by the ordinary process of the criminal law. This is not to say that a plausible national-security concern —broadly defined—is lacking in each instance of a tap. It is to say that this concern frequently serves as an *excuse* for a broad surveillance whose primary purpose is either political or conventional law enforcement.

Whether or not the civil libertarians are correct in their assessment of the value of warrants in curbing abuse, their claim that domestic national-security wiretaps have been authorized in highly questionable cases is supported by the evidence currently available. Consider, for example, the tapping of Martin Luther King's telephone (and the electronic "bugging" of his hotel rooms). These warrantless invasions of King's privacy—and the privacy of countless others who conversed with him—have been defended as necessary for the national security. But in what specific sense did the security of this nation depend on the FBI's overhearing King's telephone conversations and eavesdropping on his hotel-room activities? A number of justifications have been offered by those close to Robert Kennedy, who, as attorney general acceded to J. Edgar Hoover's request to authorize the tap. (No authorization was ever given for the bug in the hotel rooms.)

The Kennedy version goes something like this: two of King's close associates —one a New York lawyer, the other a member of the SCLC staff—were thought to be either Communist agents, party members, or sympathizers. After receiving warnings from the Justice Department that associating with these persons might damage the civil-rights movement, King dismissed the tainted staff member and initially severed his relationship with the suspected lawyer. But after a while, contact with the lawyer was gradually reestablished. It was this that led Kennedy to authorize Hoover to tap King's home phones and those in his Atlanta and New York offices.

Burke Marshall—Kennedy's respected and civil-liberties-minded assistant attorney general—has made the shocking statement that his boss may have "refused too long" to authorize the King national-security tap. "I can't tell you who the man was or what the allegations were," he says, "but I can tell you I think it would not be responsible for an attorney general—in view of the characterizations of what that man was doing and who he was working for—for the attorney general to refuse a tap." He continues, suggestively but mysteriously: "If you take it as being true that there has been an espionage system and that the Bureau has an obligation to do things about that—if you put that all together, I would say you could say he refused too long."

Very well, then, let us "take" all that as "being true." Let us assume the very worst: that the New York lawyer was a real Russian spy, working for, and being paid by, the KGB. Assume further that his sole job was to influence King in directions favored by the Soviet Union. Assume even further that he

was succeeding. Would this justify a national-security tap on King's phone? There is surely no claim that King was being used to further espionage or sabotage activities. He was, after all, engaged primarily in entirely lawful and constitutionally protected activity (even if that activity could hypothetically be shown to have favored the interests of the Soviet Union). He made and received thousands of calls to and from concerned, patriotic, and lawabiding American citizens about matters that were none of the government's business to overhear. He also engaged in—or erroneously believed he was engaged in—a private life, which also was none of the government's business to monitor. His telephone contact with the New York lawyer was an extremely small and sporadic part of his activities (and there is no evidence that he met with *him* in the bugged hotel rooms). Yet the wiretap picked up and recorded *all* of the conversations on these phones. Even if the scenario suggested by the Marshall version is accurate, should it not have been more sensible to tap the New York lawyer's phones? (Indeed, since it is technically feasible to monitor and record only calls placed between two specified numbers, it would have been possible to tap and record only those calls placed between King and the suspected lawyer.)

It is significant that a former public official as respected and dedicated as Burke Marshall would argue that it would "not be responsible" for an attorney general to have declined, or even delayed, authorization for a warrantless national-security wiretap on the basis of the evidence that he suggests existed. We only rarely have men in positions of power as sensitive and as committed to civil liberties as Marshall. If this is what we can expect of a Burke Marshall, what can we expect of the men who generally populate high office?

Another justification offered by some Kennedy intimates is that the tap was authorized, as former attorney general Katzenbach put it, "for the protection of Dr. King." Giving the FBI the power to protect King is like giving the cat the power to protect the canary. In fact, it is now widely acknowledged that no sooner did J. Edgar Hoover come up with some damaging information about King—relating to his sex life—that he leaked it to the press. Was this also done to protect King?

It is not difficult to understand what really motivated the King wiretap. The existence of the lawyer in New York provided a plausible—that is perhaps too strong a word—argument that some vague national-security interest was involved. The FBI seized upon this excuse to request authorization to do what they wanted to do for other—completely illegitimate—reasons. It was difficult for the Justive Department to deny the request: what would it look like later on if it did turn out that King was indeed involved with Communists and if Hoover leaked to his Congressional or newspaper cronies the fact that Kennedy had stood in the way of an investigation which would have disclosed this? So Kennedy took the least politically risky course. And J. Edgar Hoover got his wiretap.

The King episode does not stand alone in suggesting that the primary reason certain domestic national-security taps are employed has little to do with the genuine needs of national security. The recent case involving Muhammad Ali, which revealed the previously unacknowledged King tap, also disclosed that pervasive taps had been authorized on the phones of Elijah Muhammad, the leader of the Black Muslim Church. Here, too, I would speculate that there may have been a plausible national-security interest in a limited aspect of Elijah Muhammad's activity. But the warrantless tap was not limited, as one with a warrant would have to be. It extended to every call to and from Elijah Muhmmad's various offices over over a considerable period of time. And it picked up conversations relating to political and personal activities that were none of the government's legitimate business (for example, a disclosure that a well-known person's brother had been kicked out of the Muslim Church for being out with a girl all night).

The phrase "domestic national-security wiretap" is not self-limiting or self-defining. It means what its history tells us it means. It means what this and previous administrations have defined it to mean. Only if we are given some idea of how it has been used can the people, and the courts, have any intelligent basis for judging whether the alleged need for a domestic national-security exception outweighs its potential for abuse. On the basis of the evidence presently available, I would suggest that if we were to examine all the domestic national-security wiretaps conducted by the FBI, a disturbing picture

would emerge. We would find numerous cases where a plausible but narrow national-security concern has been used as an excuse for an improper and pervasive wiretap whose real purpose is political surveillance. Unfortunately, however, there is no way for the citizenry—or even the courts—to examine the logs of all national-security wiretaps. We are left instead with the assurances of people like former attorney general Herbert Brownell that "Experience demonstrates that the Federal Bureau of Investigation has never abused the wiretap authority."

But what "experience" is Brownell referring to? To whom has this been "demonstrated"? Certainly not to the public. I, for one, do not feel that we can rely on the self-interested assurances of former Justice Department officials that all is in order. My surmise is that if the Justice Department were to turn over the records of domestic national-security wiretaps in any given year for study to a non-partisan group of scholars, many abuses of the kind suggested above would emerge. If I am wrong—if an impartial evaluation were to disclose that warrantless domestic national-security taps have been narrowly employed only in cases of immediate, extreme, and irremediable danger to our survival—then there might be grounds for exempting this class of wiretaps from the usual constitutional requirements. But neither the people nor the courts can intelligently decide whether this is so until we are given some idea of how such wiretaps have in fact been used. In the meantime, on the basis of what we already know, we have good reason for supposing that "national security" is sometimes invoked as a pretext for political surveillance of an altogether illegitimate kind.

A Blow Struck for the Revolution

(By Jacob Marateck)

[Jacob Marateck (1883–1950) was a Polish Jew who, following a youthful career as a yeshiva student and labor agitator in Warsaw, served for a number of years in the Russian army. After a variety of adventures—including membership in the imperial bodyguard and alleged involvement in a plot to assassinate the Czar—he escaped to America. The present memoir of the Russian-Japanese War 1904–5 was taken from one of the twenty-seven handwritten notebooks kept by Marateck throughout his life; it has been adapted from the Yiddish by Shimon Wincelberg.]

The second day of Rosh Hashanah we line up for the train to Manchuria. Our lietutenant, a moody graybeard in his sixties, who ascribes his low rank to lack of "protection" at Court, tells us we're lucky. How are we lucky? We will get to ride to the battlefield in comfort, while the enemy, primitive little beasts that they are, will have to walk. He makes "battlefield" sound like a scheduled stop on the Trans-Siberian Railway. As for the "primitive" Japanese, I incline to suspect they are not exactly receiving us with open arms.

My friend Glasnick whispers I should let the lieutenant know we would also be happy to walk, and with a little luck the war will be over by the time we get there. But I'm a one-striper, a squadleader, and keep my mouth shut, scowling with authority.

The train has ninety-six cars, each packed to at least three times what it can hold. This way, the railroad is able, on one track, to deliver its quota of 30,000 replacements a month. I try not to think about the men we are "replacing."

We sit in our compartment, barely able to stir an elbow, each of us still hoarding his own fears and memories. For the moment, Russians, Ukrainians, Poles, and Jews sit packed together in a pleasnat atmosphere of revolutionary harmony. That is, somebody starts out by wondering how many of us will return alive, and soon somebody else ends up proposing that, at the next halt, we surround our officers and kill them all, then make the train go back to Petersburg and proclaim the Revolution.

No one bothers to remember that the officers have all our ammunition under lock and key. Not that it makes much difference. They're fine talkers and dreamers, our Russians, but hopelessly addicted to authority. When Glasnik wants as usual to add his comments, I quietly shut him up. I know from past experience, no matter which way the conversation turns out, they'll end up blaming it all on the Jews.

Days pass. We are all stiff and irritable from the lack of space, and no one any longer talks revolution because by now we hate the stink of one another.

But soon we come to appreciate our crowded compartments. The train has to cross Lake Baikal on rails laid over the ice, which often suddenly cracks open into yawning rifts and crevices. To keep the cars from being too heavy, the officers are taken across by horse-drawn sledge, and the rest of us walk, our rifles with their eternally fixed bayonets resting on one shoulder. Forty miles across the windswept ice, with only brief pauses for hot soup from our mobile kitchens. By morning it turns out a number of men have disappeared, probably drowned, and many more suffer from frostbite.

Another week in the unheated train, and one morning we awaken to a strange landscape in which the roofs of houses curve upward like boats, and the trees put me in mind of things that might be growing on the moon. This is Asia. The people here have darker skins and narrow, villainous Oriental eyes. Most of the men believe them already to be "Japs," having little notion that Japan is almost as far from here as Moscow.

The Orientals scatter like chickens whenever the train comes to a halt and we pile out to stretch our legs. Only some peddlers are willing to approach. The officers drive them away, they might be spies.

At one of our stops we are told to send a detail to a nearby village. They are to fetch five oxen purchased for us to slaughter for food. After a week on little but hard black bread, foul soup, and hot tea, we await their return in high spirits.

[From the Washington Evening Star, June 30, 1972]

RULED ILLEGAL BY COURT—BANNED "BUGS" TURNED OFF

(By Lyle Denniston)

Federal agnets have turned off secret listening devices that became illegal under the Supreme Court ruling against government eavesdrop policy, the Justice Department says.

The number that went out of use in the wake of yesterday's ruling was not disclosed, but the department had had just under 50 devices in use since Jan. 1, a spokesman said.

Atty. Gen. Richard G. Kleindienst ordered agents to "terminate . . . all electronic surveillance in cases involving domestic security that conflict with the court's opinion."

With no dissents, the court ruled unconstitutional the three-year-old policy of the Nixon administration for eavesdropping on "domestic subversives" without advance permission by a federal court.

The ruling was a stunning defeat for a major administration program for gathering "intelligence data" about individuals and groups whose actions it considers a possible threat to the government.

It seemed likely that the ruling would have these consequences:

A number of federal prosecutions might be dismissed because of the government's unwillingness to disclose the logs of eavesdropping made illegal by the new decision.

A series of lawsuits might be filed against the government by individuals claiming that illegal surveillance had interfered with their rights.

A period of uncertainty seemed likely to prevail until Congress reacted to a Supreme Court suggestion for new procedures to guide "domestic security" eavesdropping.

Within hours after the ruling, Kleindienst not only ordered the illegal devices turned off, but also put the Justice Department staff to work studying the pending cases which might be affected by the decision.

Kleindienst also ordered department staff members "to work closely with Congress in formulating legislative standards" that would govern court orders for eavesdropping in domestic security cases.

Since the Nixon administration came into office, federal agents have been using secret listening devices without court orders in "domestic security" cases at a rate of about 100 a year, according to the department.

A report filed with Congress last year showed that a total of 94 devices—wiretaps or hidden microphones or "bugs"—were used in 1969 and 113 in 1970 without court approval in cases involving homefront "subversives."

A department spokesman said that just under 100 were used in this category in 1971, and that, so far this year, just under 50 had been used.

SOME CASES UNAFFECTED

Kleindienst's order requiring federal eavesdropping agents to comply with the new ruling did not extend to secret devices to monitor "foreign intelligence in national security matters."

That was because the Supreme Court, in its new decision, expressly declined to rule on the legality of government surveillance without a court order in cases involving "activities of foreign powers, within or without this country."

SOME FLEXIBILITY

Presumably, that left the Justice Department with some flexibility in deciding which domestic "subversives" it still could monitor on the theory that they had had some "significant connection" with a foreign government or agency.

In the case which the Supreme Court decided yesterday, the justices concluded that the surveillance was illegal since "there is no evidence of any involvement, directly or indirectly, of a foreign power" with the man whose conversations had been overheard by a wiretap—Lawrence R. "Pun" Plamondon, a member of the White Panther party accused of bombing a Central Intelligence Agency office in Ann Arbor, Mich., on Sept. 29, 1968.

Some department officials believed that "not very many" cases would be affected. However, it seemed possible that the ruling could affect some of the more controversial cases the administration has filed—including the Berrigan bombing-kidnap conspiracy, several cases involving the Black Panther party, some cases involving the bombing of the U.S. Capitol last year, and several growing out of last year's Mayday anti-war outbreak here.

Another problem facing the government was the possibility that a number of persons involved in other controversial cases—like the Pentagon Papers' disclosure case—could make a series of new demands for any revelation of illegal eavesdropping.

In reaching their decision, the justices did make one possible gesture toward government eavesdropping policy: It ruled that Congress could make it easier to get court approval for eavesdropping in domestic security cases than in "ordinary" criminal cases.

Specifically, it suggested that Congress might want to permit courts to issue eavesdropping orders on less definite evidence than would be required for a normal criminal case; that the eavesdropping might be allowed to continue for periods longer than the initial 60 days, plus 30-day extensions, provided for under the 1968 law; that the power to issue orders be confined to one court rather than shared by all federal courts in the nation; and that the government need not be bound by the 1968 law's provision requiring public reports of eavesdropping 30 days after an approved monitoring has ended.

ALL ARGUMENTS REJECTED

The justices rejected all five major arguments the government had made to defend its eavesdropping policy:

That the president and the attorney general had sole authority under the Constitution to decide when to use eavesdropping in any national security case; that they should have this power because they would use it "reasonably;" that they should have this authority because they would use it only to gather intelligence data, not criminal evidence; that courts did not have the knowledge or background to act on security investigations, and that national security might be imperiled if courts or court personnel "leaked" data about security investigations.

The court's ruling on surveillance was the most far-reaching action it took yesterday as it continued to work toward summer adjournment. The justices scheduled another session for Thursday to issue more opinions.

[From the Washington Post, June 20, 1972]

Court Curbs Wiretapping Of Radicals

(By John P. MacKenzie)

A unanimous Supreme Court rejected yesterday the Nixon administration's claim that the Executive Branch may wiretap suspected "domestic" radicals without a court warrant.

In a major rebuff to an important administration law enforcement policy, the court held that freedom for private dissent "cannot safely be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch."

The blow was delivered by one of President Nixon's own appointees to the court, Lewis F. Powll Jr., writing for himself and five other justices. Concurring separately were Chief Justice Warren E. Burger and Justice Byron R. White.

Beginning in the 1969 prosecution of the "Chicago 8" conspiracy defendants, one of many cases vitally affected by yesterday's decision, the Justice Department asserted that judicial supervision was not required when the President and Attorney General deemed a specific wiretap necessary for protection against subversion from within.

But Powell, despite past public support for wiretapping and a reputation for concern over national security, said the Justice Department had failed to make out a case for "the time tested means" of judicial warrants for safeguarding Fourth Amendment guarantees against unreasonable searches and seizures.

Presidents since Franklin D. Roosevelt have asserted the power to conduct electronic surveillance against suspected foreign agents without permission from a court but it was not until John N. Mitchell became Attorney General that the government claimed similar authority concerning home-grown radicals who were not accused of acting as foreign-supported spies or revolutionaires.

Emphasizing that the foreign agent problem was not before the high court, Powell said that even the domestic issues pressed by the department "merit the most careful consideration" when urged "on behalf of the President."

"We do not reject them lightly," said Powell, "especially at a time of worldwide ferment and when civil disorders in this country are more prevalent than in the less turbulent periods of our history."

Powell then went on to reject every administration argument, including the contention that internal security matters are "too subtle and complex" for judges.

"There is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases," Powell said, adding:

"If the threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probably cause for surveillance."

Powell denied that there was significant danger of compromising intelligence secrets when government lawyers must go secretly to a court for warrants.

He noted that Congress, in passing wiretapping legislation in 1968, already had imposed a sensitive responsibility on judges by authorizing wiretapping and bugging warrants in espionage, sabotage and treason investigations.

"Although some added burden will be imposed upon the attorney general, this inconvenience is justified in a free society to protect constitutional values . . . By no means of least importance will be the reassurance of the public generally that indiscriminate wiretapping and bugging of law-abiding citizens cannot occur."

Powell said public uneasiness was justified by the "danger to political dissent" inherent in the vague concept of national security, since "the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs."

He added, "The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power."

The reassurance stems from the independent judgment of a neutral and detached magistrate who determines whether there is a reasonable basis for the electronic intrusion upon privacy, Powell said.

He indicated that under appropriate guidelines for such warrants, the government might have been able to obtain approval to eavesdrop on Lawrence

(Pun) Plamondon, a leader of the radical White Panther Party accused of conspiring to blow up a Central Intelligence Agency building at Ann Arbor, Mich.

Lower courts ruled that wiretap records in the case must be turned over for defense inspection to see whether the illegal taps produced part of the prosecution's case. Yesterday's decision forces the government to choose between disclosure to the defense and abanodning the prosecution in the Ann Arbor case, the Chicago case now on appeal, and numberous others.

Powell offered a suggestion that Congress might enact special standards for the warrants, perhaps allowing agents to install listening devices for longer periods than provided in the 1968 law for conventional crime investigations.

He totally rejected the government's argument that Congress had immunized domestic radical taps from the warrant requirements.

Attorney General Richard G. Kleindienst said last night that he is terminating all domestic security wiretaps that conflict with the court's opinion. He said his staff would work with Congress to seek new warrant standards in line with the court's suggestion.

Joining Powell were Justices William O. Douglas, William J. Brennan Jr., Potter Stewart, Thurgood Marshall and Harry A. Blackmun. Burger noted simply that he concurred "in the result" and White based his concurrence on language in the 1968 act.

Justice William H. Rehnquist, who helped shape the government's arguments as a Justice official last year, did not participate.

[From the New York Times, June 20, 1972]

High Court Curbs U.S. Wiretapping Aimed at Radicals—Rules Warrant Is Necessary for Federal Surveillance in Domestic Matters

(By Fred P. Graham)

Washington—The Supreme Court declared unconstitutional today the Federal Government's practice of wiretapping without first obtaining court approval, domestic radicals considered dangerous to the national security.

The Court, 8 to 0, rejected the Nixon Administration's assertion that the President's authority to protect the nation from internal subversion gives the Government the constitutional power to wiretap "dangerous" radical groups without obtaining court warrants.

"Fourth Amendment freedoms [against "unreasonable searches and seizures"] cannot properly be guaranteed if domestic surveillances may be conducted solely within the discretion of the executive branch," the Court declared.

JUSTICE AGENCY SETBACK

Without ruling on the constitutionality of warrantless wiretapping against agents of foreign powers, the Court held that "national security" wiretapping of domestic radicals who have no foreign ties can be done only with the type of court warrants currently used in police wiretapping of organized crime.

The ruling was stunning legal setback for the Justice Department, which failed to muster a single vote from a Court with four justices appointed by President Nixon.

Attorney General Richard G. Kleindienst announced after learning of the decision that he had "directed the termination of all electronic surveillance in cases involving security that conflict with the Court's opinion." He said that subsequent surveillance would be done "only under procedures that comply" with the decision.

The opinion was written by Justice Lewis F. Powell Jr., who was appointed to the Court shortly after he wrote a newspaper article strongly supporting the President's "national security" wiretap power.

FEAR OPPOSED AS PRICE

Justice Powell had termed the complaints against the Government's wiretapping "a tempest in a teapot" and had suggested that the distinctions between warrantless wiretapping of foreign agents and domestic subversives was

"largely meaningless." But he assured the Senators at his confirmation hearing that his mind was still open.

His opinion today leaned heavily upon the threat to free speech that he saw in unbridled governmental wiretapping of dissenters.

"History abundantly documents the tendency of government—however benevolent and benign in its motives—to view with suspicion those who most fervently dispute its policies," he wrote.

"The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power," he continued. "Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation."

Justice William H. Rehnquist, another Nixon appointee who had made statements supporting the President's wiretap authority before joining the Court, did not participate in the decision. He had suggested that he would participate by remaining behind the bench when the case was argued. He gave no reason for stepping aside today.

By coincidence, the historic decision was announced only seconds after Attorney General Kleindienst, an aggressive proponent of warrantless wiretapping, formally presented the Supreme Court his credentials as the Government's chief legal officer.

Mr. Kleindienst, clad in the cutaway coat and striped trousers customarily worn by Government attorneys in the Supreme Court, was welcomed by Chief Justice Warren E. Burger in a brief statement as the Court session began.

KLEINDIENST LEAVES

Then as the Justices settled back for thte announcement of the first decision, Mr. Kleindienst strode from the courtroom, not waiting long enough to hear that the long-awaited wiretapping ruling was about to be handed down.

An important result of the decision is that any defendant in a Federal prosecution has a right to see complete transcripts of any conversations overheard on a warrantless "domestic security" listening device so that his lawyer can make certain that no illegally obtained information is being used by the prosecution.

Court records indicate that victims of such wiretapping could include defendants in the "Chicago Seven" riot-conspiracy case, the kidnapping conspiracy case involving the Rev. Philip F. Berrigan and other prosecutions of antiwar activists and black radicals.

Mr. Kleindienst said that his staff would screen all such cases to decide whether to disclose the wiretap transcripts or drop the prosecutions.

Today's ruling had its roots in a decision by President Roosevelt in 1940 that he had the power to wiretap suspected German spies. In 1946, President Truman broadened the practice to include American citizens suspected of espionage.

It was not until 1967, when the Supreme Court ruled that electronic surveillance was subject to the Fourth Amendment's warrant requirements, that the Government was confronted with the issue of what to do about this type of "national security" surveillance.

In 1968 Congress passed a law authorizing law enforcement officers to get court warrants to investigate a wide variety of crimes. The law stated that it would not affect any constitutional authority the President might have to wiretap in national security cases without warrants.

This confronted the Nixon Administration with the choice of trying to obtain court warrants for its national security surveillance or to take the chance that the Supreme Court would uphold warrantless eavesdropping.

LATTER COURSE TAKEN

Attorney General John N. Mitchell took the latter course—one so controversial among career attorneys that when the case reached the Supreme Court no member of the Solicitor General's office argued the Government's case.

Robert C. Mardian, then Assistant Attorney General in charge of the Internal Security Division, made the argument. He was opposed by Arthur Kinoy of the Center for Constitutional Rights in New York, and William T. Gossett of Detroit.

Mr. Kinoy represented three members of the radical White Panther party who were accused of plotting to bomb a Central Intelligence Agency office in Detroit. Mr. Gossett argued for United States District Judge Damon Keith, who ordered the Justice Department to disclose the transcripts of the defendants' conversations obtained by wiretaps installed without court permission.

The United States Court of Appeals for the Seventh Circuit upheld Judge Keith.

Justice Powell's opinion held that the 1968 statute did not give the Government the power to wiretap without court authority, but merely left untouched any constitutional power it might have had anyway.

He stressed that the Court was leaving for another day a decision on whether warrants will be required to wiretap foreign spies and that the decision today covered only those with "no significant connection with a foreign power, its agents or agencies."

Justice Department officials are expected to argue that many of the radicals who have been wiretapped have had contacts with Communist countries, and the ruling could make left-wing groups more circumspect about their future dealing with foreign governments.

Legal experts disagree as to whether the Government can obtain warrants under the 1968 act for surveillance of radicals, because the Government must show probable cause that a specific law is about to be violated. National security surveillance is usually based upon more nebulous suspicions.

Justice Powell's opinion virtually invited Congress to pass a new law to allow for this special type of wiretapping, but any proposal so loaded with overtones of political surveillance would be expected to face difficulty on Capital Hill.

Chief Justice Burger noted that he concurred only in the result. Justice Byron R. White, in a separate concurring opinion, said that the warrantless surveillance might have been legal under the "national security" exception of the 1968 law, but that the Justice Department's Court papers did not satify the statute.

LIBERTIES UNION STATEMENT

In New York today, the American Civil Liberties Union hailed the wiretapping decision. A statement by the organization's executive director, Aryeh Neier, said:

"The Supreme Court has rejected the Government's boldest claim of powers to intrude upon individual liberties. The Government had claimed that in the undefined interests of 'national security' it could engage in a vast, lengthy, unsupervised and unchecked invasion of the privacy of people having only the remotest link with anything in any way criminal or even wrong.

"If this claim had been upheld, there would have been virtually no limits to the range of governmental intrusion on liberty that would have been implicitly authorized once the Government invoked the talisman of 'national security.'

"In rejecting the Government's claims, the Court has vindicated the constitutional liberties of all Americans."

[From the New York Daily News, June 20, 1972]

TOP COURT LIMITS WIRETAPS

(By Jeffrey Antevil)

WASHINGTON.—In a major rebuff to the Nixon Administration, the Supreme Court rejected unanimously today the Justice Department's argument that the government can legally wiretap suspected domestic "subversives" without first getting a court order.

Declaring in a Michigan case that such bugging without a warrant is unconstitutional, Justice Lewis F. Powell wrote for the court that "unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy."

Former Attorney General John N. Mitchell, who brought the test case to the high court, argued that the individual's right to privacy must yield to the government's need to defend itself against potential threats to the national security. Thus, he said, the government has the power to eavesdrop on sus-

pected domestic subversive groups without prior judicial approval, just as it does in foreign intelligence cases.

CALL CONCEPT VAGUE

Powell, a Nixon appointee, declared in an opinion joined by justices William O. Douglas, Thurgood Marshall, Potter Stewart, Harry A. Blackmun and Wilaim J. Brennan Jr. that "the danger to political dissent is acute where the government attempts to act under so vague a concept as the power to protect 'domestic security'."

"The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power," Powell added.,

Chief Justice Warren E. Burger and Justice Byron R. White wrote separate opinions agreeing with the majority action in the case of Lawrence Plamandon, a member of the now-defunct White Panther Party who was accused of conspiring to blow up CIA offices in Ann Arbor, Mich. Justice William H. Rehnquist, an assistant attorney general until this year, did not participate in the case.

LOWER COURT ORDER

Two lower court judges, rejecting the government's position, had ordered transcripts of wiretaps of Plamandon's conversations turned over to his lawyers.

The Justice Department has continued to wiretap other domestic militant groups, such as the Wetherman faction of the Students for a Democratic Society, while its appeal was pending.

In other action today, the court:

Agreed with New York's claim, in a dispute with Pennsylvania over $1.5 million in uncashed Western Union money orders, that the money belongs to the state where the person entitled to claim it was last known to live.

Agreed to consider next term New York's claim that complaints by state prison inmates about their treatment should be made in state, not federal courts.

Ruled in an Arkansas case that a man acquitted of a murder charge cannot, under the constitutional ban against doubel jeopardy, be tried for robbery in the same incident.

Agreed to rule next term whether its 1969 decision barring court-martial trials of servicemen for non-service-related offenses should be made retroactive to clear the records of thousands of former servicemen convicted before that date.

Upheld a law in Florida allowing a municipal clerk who is not a judge to issue arrest warrants.

[From the New York Times, June 22, 1972]

KLEINDIENST SEES A DECLINE IN WIRETAPS

(By Fred P. Graham)

WASHINGTON.—Attorney General Richard G. Kleindienst said today that last Monday's Supreme Court decision on wiretapping would reduce the Government's intelligence about subversive activities, "but not to an extent that will damage our national security."

The Supreme Court held that the Government must obtain court warrants before wiretapping may be used against allegedly subversive radical domestic groups. For at least 26 years, the Government had been wiretapping such groups without court permission.

Mr. Kleindienst said in an interview that the ruling, would cut down on eavesdropping for intelligence-gathering purposes because the Federal law on wiretapping requires proof that a crime has been or is about to be committed before Government agents will be given a warrant to eavesdrop.

'NOT A DEAD-END STREET'

But he said the 8-to-0 decision 'is not a dead-end street for electronic surveillance because the Government could request warrants when a radical group appeared to be planning a specific crime.

He said the Justice Department would cooperate with Congress in drawing up a new wiretapping law to permit court warrants in "domestic security" situations that were not clearly covered under the present law.

Mr. Kleindienst said that as soon as he read the Supreme Court's opinion last Monday, he asked the Federal Bureau of Investigation for an inventory of internal security wiretaps then in use without warranty.

There were "less than 30," he said. Of these, he said, "less than 10" were considered to be directed at groups that were not significantly involved with foreign power. Mr. Kleindienst said all of these had immediately been turned off.

He declared that the Justice Department would not attempt to continue eavesdropping on domestic groups without warrants by contending that the groups had foreign ties. The Supreme Court ruling left it undecided whether the Government might continue to wiretap without court approval where foreign intelligence was involved.

MITCHELL SIMILARITY SEEN

Mr. Kleindienst's statements were made during a luncheon with members of the Washington Bureau of The New York Times.

Mr. Kleindienst, who was sworn in as Attoreny General earlier this month, said there would not be "too much of a difference" between his Justice Department and that of his predecessor, John N. Mitchell.

He said that Mr. Mitchell had accomplished more than his Democratic predecessors in civil rights but that under the Kleindienst regime "more emphasis on civil rights enforcement" than was evident under Mr. Mitchell could be expected.

He also said that there would be "a much more intensive program of penology reform.

He disclosed that he and his family had been involved in efforts to rehabilitate two young men who would otherwise have been sent to prison. To protect their privacy, Mr. Kleindienst declined to give more details.

Mr. Kleindienst said he would not make policital speeches or criticize the Democratic candidate during the Presidential campaign. Instead, he said, he will "go around the country telling the accomplishments of this Government in the justice area."

But he conceded that the Democrats could legitimately appointment. He said he would expect the Democratic nominee to say in his acceptance speech: "I will give you a new Attorney General—who won't sell out to I.T.T."

This was an allusion to Richard M. Nixon's pledge, in his acceptance speech at the 1968 Republican convention, to name a new Attorney General to replace Ramsey Clark. Some Democrats tried to block Mr. Kleindienst's confirmation by alleging that he had been improperly involved in the settlement of three antitrust suits against the International Telephone and Telegraph Corporation—a charge he denied then and again in the interview today.

[From Newsweek Magazine, July 3]

THE SUPREME COURT: UNTAPPED

It was three years ago that the Nixon Administration first enunciated the principle that domestic "radicals" were fair game for government bugging and wiretapping—without prior court approval—in the interests of national security. That policy quickly became a hallmark of John Mitchell's Justice Department and the focus of mounting protests and paranoia on the left. But last week, in a stunning 8-to-0 decision, the Supreme Court rebuked the Administration and declared the practice unconstitutional. "The fear of unauthorized official eavesdropping [must not] deter virgorous citizen dissent," said the High Court. "For private dissent, no less than public discourse, is essential to our free society."

The decision constituted a historic reaffirmation of the First and Fourth Amendments—the right to free speech and the guarantee against unreasonable search and seizure. Beyond that, it was a sharp reminder of how unpredictable the Supreme Court can be—even to a President who had handpicked four of the nine Justices to complement his own tough views on law, order and the

limits of dissent. Civil libertarians, of course, greeted the ruling with wholehearted enthusiasm, and the Justice Department immediately began pulling the plug on those few of its snooping operations that it admitted fell under the new prohibition. Perhaps more important, the department has to consider how to go ahead with similar surveillance in the future—and whether to drop a sizable number of cases now pending.

CLAIM

Eavesdropping in the interest of domestic security has been going on at least since Harry S. Truman's Administration. What distinguished the Nixonians from their predecessors was that they not only did it but said so—and in fact claimed it as a perfectly legitimate exercise of government power. The controversy, and the claim, surfaced when the Administration admitted having listened in on some of the Chicago Eight, the odd-lot assortment of radicals charged with having incited rioting at the 1968 Democratic convention. The government relied heavily on the Safe Streets Act of 1968, which specifically exempted from regulation any authority the President might have to order taps in security cases. This, said the Administration, meant not just agents of foreign powers but domestic subversives as well.

Ironically, last week's Supreme Court decision knocking down that broad-gauge definition of "national security" was delivered by Justice Lewis F. Powell Jr., who had strongly supported the practice prior to his nomination by President Nixon. Powell promised senators at his confirmation hearings that he would keep an open mind on the question, and his closely reasoned opinion demonstrated that he had. The case at hand involved Lawrence Robert (Pun) Plamondon, a member of the radical White Panthers, who was charged with dynamiting offices of the Central Intelligence Agency at Ann Arbor, Mich., in 1968. As in the Chicago Eight case, the government admitted that some of Plamondon's conversations had been overheard by agents tapping the phones of an undisclosed organization for security purposes. And againt it claimed that such surveillance, without a warrant, was legal under language in the Safe Streets Act. But Federal District Judge Damon J. Keith in Detroit disagreed and ordered transcripts of any illegal taps turned over to the defense.

Justice Powell upheld the district judge, ruling that Congress had not given the President any wiretap power but only refused to limit whatever authority he might already have under the Constitution. Powell left aside the question of snooping on foreign agents, or U.S. citizens significantly involved with a foreign power. But he held that a proper balance between national security on the one hand, and the constitutional right to privacy and free speech on the other, demanded a decent respect for established search-warrant procedures in domestic cases. "Fourth Amendment freedoms cannot properly be guaranteed," Powell wrote, "if domestic security surveillances may be conducted solely within the discretion of the executive branch." He also found, government arguments to the contrary, that judges were perfectly capable of keeping secrets and of understanding security cases. "If the threat is too subtle or complex for our senior law-enforcement officers to convey its significance to a court," he remarked tartly, "one may question whether there is probable cause for surveillance."

Attorney General Richard Kleindienst, a vigorous proponent of wiretapping domestic "subversives," reacted quickly once the ruling was issued. He ordered the termination of "all electronic surveillance . . . that conflicts with the Court's opinion" (fewer than a dozen cases, according to a spokesman) and announced that the department would work with Congress to develop reasonable standards for warrants in national security cases. It also seemed likely that the government would place greater emphasis on the foreign ties forged by many domestic radicals with Cuba, Hanoi and North Korea. But the most immediate question raised by last week's decision was whether to turn over potentially embarrassing wiretap transcripts in a score or so of important cases already pending—or drop the prosecutions. Among the defendants: Chicago Eight alumni Abbie Hoffman and David Dellinger and antiwar priest Philip Berrigan.

[From Time Magazine, July 3]

NEW CURB ON BUGGING

Shortly after taking office, the Nixon Administration claimed the right to eavesdrop—without a judicial warrant—on anyone it chose to consider a threat to the national security. By the time the issue reached the Supreme Court, Nixon had appointed four new Justices, so the Government thought its chances of enforcing the claim seemed promising. But last week, by a vote of 8 to 0, with Justice William Rehnquist abstaining, the court declared that bugging or tapping domestic political "suspects" without a warrant is illegal. "Those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks," said Justice Lewis Powell.

The Administration's failure to make a case was highlighted by the fact that Powell wrote the court's opinion. Just last year, when Powell was a lawyer in private practice, he wrote that "the outcry against wiretapping is a tempest in a teapot. Law-abiding citizens have nothing to fear." From his new vantage point on the Supreme Court, however, Powell found that the Government's electronic surveillance was not "a welcome development—even when employed with restraint."

TOO COMPLEX

The Justice Department had wanted to avoid the Fourth Amendment's rule on warrants because it uses electronic devices to gather general intelligence on various political groups, and it argued that its reasons for doing so are too "complex and subtle" for a judge to evaluate competently. Powell responded sharply: "If the threat is too subtle or complex, one may question whether there is probable cause for surveillance. . . . The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power."

Powell did not deal, however, with warrantless eavesdropping on foreign agents, which the Government has felt free to do ever since President Roosevelt authorized taps on suspected spies during World War II. "No doubt," said Powell, "There are cases where it will be difficult to distinguish between 'domestic' and 'foreign' activities directed against the Government. But this is not such a case."

Specifically, the case before the court involved Lawrence ("Pun") Plamondon, a member of a left-wing organization called the White Panthers, who was accused of bombing a CIA office in Ann Arbor, Mich. The Administration did not contend that any foreign government was involved, and therefore, the court ruled, there was no question that Plamondon was protected by the Fourth Amendment.

Attorney General Richard Kleindienst appeared unfazed by the court's decision. "I asked the FBI to compile a list of surveillance devices yesterday afternoon, and they should all be pulled by now," he told TIME's David Beck- ??? Line Missing in Copy ??? with the day after the decision. How many such devices were there? "Very few. You could probably count them on the fingers of both hands. We only used them where we thought there was a threat of violence. I had just authorized a couple more last week, but I'm not going to talk about any individual taps. If I say anything, they [defendants and suspects] will come in and ask for transcripts of everything we took."

NO BLEEDING HEART

Kleindienst was referring to a Supreme Court ruling three years ago which declared that individuals subjected to illegal eavesdrops have a right to transcripts of what has been overheard if they are to be prosecuted. Warrantless taps are known to have been used, for example, in investigations of the Chicago Seven and in the recent Berrigan case. Wherever violations are found, the Justice Department will have to either disclose the details of the eavesdropping or drop prosecution. Wouldn't it be only proper to inform anyone who has been illegally overheard? "Hell, no," said Kleindienst. "Our duty is to prosecute persons who commit crimes. We don't have to confess our sins anywhere, like some bleeding heart. We were acting in good faith."

What paths will the Administration now follow? The President at his press conference said that no legislation would be sought to eliminate the warrant

requirement. Other Administration sources, however, were interested by a suggestion in the court's opinion that Congress could establish different and presumably easier standards for issuing warrants in security cases.

Meanwhile, according to a spokesman for Justice's Internal Security Division, "the ruling will make the division's job a little more difficult, but it certainly doesn't put it out of business. We took the position before the court that you cannot separate foreign from domestic threats, and we still believe that. It's a fine line, one that the court could only define as "no significant connection with a foreign power.' I imagine that we will consider any real connection to be 'significant' until we're instructed otherwise."

[From the Wayne Law Review, Vol. 14, 1968]

The "National Security" Justification for Electronic Eavesdropping: an Elusive Exception

(By Athan G. Theoharis† and Elizabeth Meyer††)

I

THE ARGUMENTS

Electronic surveillance and wiretapping are today's more sophisticated forms of the ancient practice of eavesdropping. Although the subject of innumerable pages of comment, congressional hearings and recent Supreme Court decisions, the state of the law remains essentially as it was in 1934, unclear. The Supreme Court, in *Katz v. United States*,[1] clarified the area in one respect: electronic eavesdropping is not per se unconstitutional. A decision remains to be made with respect to the situations in which electronic eavesdropping is, and is not, appropriate.

The Constitution does not specifically prohibit electronic eavesdropping as a method of police investigation; it merely regulates the police methods, as illustrated by the concern, especially of the recent cases,[2] with the procedural questions of the search warrants issued. Serious constitutional objections to the use of electronic eavesdropping have been raised, and the desirability of such an investigative technique must be determined in the light of these objections. Various legal and psychological arguments have been made against eavesdropping, but whatever their orientation, they place a high value on the individual's right of privacy and abhor the "dirty business" [3] of eavesdropping. The legal arguments generally are based upon alleged violations of the first, fourth, fifth and sixth amendments of the Constitution. The eavesdropping critics advocate the application of an exclusionary rule to regulate police practices [4] where it is found that eavesdropping infringes upon these rights.

It is contended that electronic surveillance violates the first amendment by creating a prior restraint on free speech; [5] a person, aware that someone else might be monitoring his conversation and recording his words, is afraid to speak candidly. Typically, this argument is answered by the contention that the innocent person has nothing to fear. However, the prior restraint objection has

---

† Assistant Professor of History, Wayne State University, B.A. 1956, B.A. 1957, M.A. 1959 in Political Science, Ph.D. 1965 in History, University of Chicago.

†† Senior editor, Wayne Law Review; B.A. 1965, Kalamazoo College; J.D. 1968, Wayne State University.

The authors wish to express appreciation to Wayne State University and the Truman Institute for National and International Affairs, the research facilities of which made this article possible.

[1] 389 U.S. 347 (1967).

[2] E.g., Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967); Osborn v. United States, 385 U.S. 323 (1966).

[3] Olmstead v. United States, 277 U.S. 438, 470 (1928) (Holmes, J., dissenting).

[4] Aspen, Court-Ordered Wiretapping: An Experiment in Illinois, 15 DePaul I. Rev. 15, 16-17 (1965); Comment, On Applying the "Mere Evidence" Rule to Government Eavesdropping, 14 U.C.L.A.L. Rev. 1110 (1967).

[5] Schwartz, The Wiretapping Problem Today, 2 Crim. L. Bull., Dec. 1966, at 3; King, Wiretapping and Electronic Surveillance: A Neglected Constitutional Consideration, 66 Dick. L. Rev. 17, 25-30 (1961); King, Electronic Surveillance and Constitutional Rights: Some Recent Developments and Observations, 33 Geo. Wash. L. Rev. 240, 266-67 (1964); Note, Eavesdropping and the Constitution: A Reappraisal of the Fourth Amendment Framework, 50 Minn. L. Rev. 378, 397-400 (1965).

considerable contemporary significance when the possibility of electronic eavesdropping is considered in the context of the current upsurge in political reaction, dissent and recent overt attempts to stifle criticism of the administration's foreign policy.[6] The value of free dissent in a democratic society is so substantial that the objection to the subtle propensities of electronic eavesdropping is significant.

The fourth amendment provides that a magistrate may issue a search warrant upon a showing of probable cause and requires that the objects which are to be seized be specifically and particularly described. The indefiniteness of words and the indiscriminate nature of any warrant issued form the basis of the fourth admendment eavesdropping problem.[7] The objection is that in the course of the investigation much irrelevant and innocent conversation will be transcribed since it is impossible to determine at what precise moment the words which are meaningful to the investigation might be uttered. Thus, it is contended that wiretapping is an unreasonable exploratory search and seizure.

The fifth amendment objection arises when the words are recorded in order to be replayed later as evidence at trial.[8] Thus, the person incriminates himself not by virtue of statements made with full knowledge of the circumstances under which and to whom they were being made, but by mechanical reproduction of his own words surreptitiously gathered. The trend of modern decisions involving the fifth amendment has been toward eliminating the reliance upon incriminating statements made by the defendant.[9] These fifth amendment arguments are bolstered by the invocation of the right to counsel protected by the sixth amendment.[10] It is contended that the use of incriminating statements recorded after the investigation has focused upon the defendant denies him the benefit of effective advice of counsel.

The final legal argument is that electronic eavesdropping is proscribed by the penumbra theory of *Griswold v. Connecticut*.[11] The essence of this theory is that the Bill of Rights' guarantees create a constitutionally protected zone which is banned from police intrusion. Since the essential character of all the objections is the right to privacy, it is sometimes contended that this area comes within the protective zones of privacy established in the *Griswold* case.[12] The value of privacy as concerns the psychological needs of the individual forms the basis for an additional objection to electronic eavesdropping. These needs, in Professor Westin's formulation,[13] are "personal autonomy," [14] "emotional release," [15] and "limited and protected communication." [16]

---

[6] An example of this is General Hershey's letter to local draft boards on Vietnam war protestors. N.Y. Times, Nov. 8, 1967, at 1, col. 2; id., Nov. 9, 1967, at 2, col. 4.

[7] Other fourth amendment objections are the failure to obtain any warrant at all and the tendency of magistrates to merely rubberstamp all warrant requests. See generally Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967); Silverman v. United States, 365 U.S. 505, 512 (1961) (Douglas, J., concurring); Semerjian, Proposals on Wiretapping in Light of Recent Senate Hearings, 45 B.U.L. Rev. 216, 223-29 (1965); Hines, Fourth Amendment Limitations on Eavesdropping and Wiretapping, 16 Cleve.-Mar. L. Rev. 467 (1967); Schwartz, supra note 5, at 9-12; Donnelly, Electronic Eavesdropping, 38 Notre Dame Law. 667 (1963); Comment, Eavesdropping Orders and the Fourth Amendment, 66 Colum. L. Rev. 355 (1966); Comment Eavesdropping, Informers and the Right of Privacy: A Judicial Tightrope, 52 Cornell L.Q. 975, 985-89 (1967); Note, Eavesdropping and the Constitution: A Reappraisal of the Fourth Amendment Framework, 50 Minn. L. Rev. 378, 400-13 (1965); Comment, A New Constitutional Limit for Electronic Surveillance Cases, 7 Wm. & Mary L. Rev. 93 (1966); cf. Lopez v. United States, 373 U.S. 427, 463 (1963) (Brennan, J., dissenting).

[8] Hines, supra note 7, at 468; King, supra note 5, at 265-66; Note, supra note 7, at 400-13; Comment, A New Constitutional Limit for Electronic Surveillance Cases, 7 Wm. & Mary L. Rev. 93 (1966).

[9] E.g., Miranda v. Arizona, 384 U.S. 436 (1966); Escobedo v. Illinois, 378 U.S. 478 (1964).

[10] Comment, Electronic Surveillance, 17 Baylor L. Rev. 338, 352-53 (1965); Note, supra note 7, at 400-08.

[11] 381 U.S. 479 (1965); see Katz v. United States, 389 U.S. 347, 350 n.4 (1967); 40 St. John's L. Rev. 59, 65 (1965).

[12] Closely related to this theory, and perhaps an unconscious underlying basis for it, is the apprehension of abuse of the recorded surveillance. The feared abuses are tampered tapes and the possibility of extortion. President's Commission on Law Enforcement and Administration of Justice, Task Force Report on Organized Crime 98 (1967).

[13] A. Westin, Privacy and Freedom 32-42 (1967).

[14] This concept refers to the need to protect a central core of the individual's personality from public divulgence.

[15] The individual needs to have "emotional release" as a safety value of sanity to vent his frustrations in the form of angry attack on the system.

[16] Confidential relationships must be allowed in order to enable the person to choose a limited group with which he can share his "secrets" without being forced to conceal everything of personal importance from all others.

Proponents of the use of electronic eavesdropping contend that while there are valid objections concerning the individual's rights, countervailing societal interests must be taken into account. Initially the inadequacies of more orthodox police techniques to satisfy the needs of efficient administration of justice with respect to highly secretive, conspiratorial crimes and espionage [17] must be considered. It is argued that electronic eavesdropping is warranted in at least some cases to give the police an adequate tool to combat sophisticated organized crime. These crimes are generally conspiratorial with a hierarchy of participants; the leaders never actually participate in the crimes committed, and it is difficult to gather incriminating evidence without electronic eavesdropping.[18] Further justification is based upon the oft cited contention that without wiretapping New York would never have convicted James "Jimmy" Hines, John Paul Carbo, Charles "Lucky" Luciano, and Anthony Carfano, all important members of organized crime.[19]

Another argument with respect to the inadequacy of orthodox police methods is based upon the fact that the conspirators often communicate without meeting together. Robert Kennedy, when Attorney General, testified before the Senate Judiciary Committee that the Cosa Nostra, for example, uses the telephone extensively and that the Apalachin (New York) type of meeting is a rare occurrence.[20] Moreover, informers courageous enough to testify in open court are extemely rare.[21] To these factors are attributed the Cosa Nostra's success in avoiding prosecution, and these same factors are used as supportive evidence by proponents of legalized eavesdropping when referring to the need of the police to use electronic devices.[22]

The authors believe that, in light of the serious constitutional objections which have been raised and the competing social needs, the use of electronic eavesdropping can be condoned only where ordinary police techniques have failed.[23] In the areas of organized crime and espionage directed by a foreign government the threat is serious enough and ordinary police methods inadequate enough to countenance the use of electronic eavesdropping. Only in these two areas is a balance between individual rights and investigatory leeway reached and a statute should be passed to codify this balance, providing for limited electronic surveillance.

II

THE HISTORICAL DEVELOPMENT OF WIRETAP POLICY

In spite of historically separate treatment by the Court, wiretapping and electronic eavesdropping are basically similar in nature. This is demonstrated by the Court's recent failure to distinguish between the two in *Berger v. New York* [24] and *Katz v. United States*.[25] Wiretapping, subject to the same constitutional limitations as other forms of electronic eavesdropping, is, in addition,

---

[17] Brown, The Great Wiretapping Debate and the Crisis in Law Enforcement, at N.Y.L.F. 265, 273 (1960); Brown & Peer, The Wiretapping Entanglement: How to Strengthen Law Enforcement and Preserve Privacy, 44 Cornell L.Q. 175 (1959); Lumbard, The Lawyers' Responsibility for Due Process and Law Enforcement, 12 Syracuse L. Rev. 431, 441 (1961); Lumbard, Wiretapping and Senate Bill 675, 5 Am. Crim. L.Q. 130 (1967), Silver, The Wiretapping-Eavesdropping Problem: A Prosecutor's View, 44 Minn. L. Rev. 835, 848-49 (1960); Comment, A Federal Wiretap Law—Needed Weapon Against Organized Crime, 13 DePaul L. Rev. 98, 109-10 (1963); Note, Electronic Surveillance and the Right of Privacy, 27 Mont. L. Rev. 173, 175-76 (1966).

[18] President's Commission on Law Enforcement and Administration of Justice, supra note 12, at 92.

[19] Hearings on S. 1086 Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary, 87th Cong., 1st Sess. 432 (1961); see Berger v. New York, 388 U.S. 41, 61-62 (1967); Aspen, Court-Ordered Wiretapping: An Experiment in Illinois, 15 DePaul L. Rev. 15, 18-19 (1965); Comment, A Federal Wiretap Law—Needed Weapon Against Organized Crime, 13 DePaul L. Rev. 98, 101 n.6 (1963).

[20] Hearings on S. 2813 & S. 1495 Before the Senate Comm. on the Judiciary 87th Cong., 2d Sess. 12 (1962).

[21] Hearings pursuant to S. Res. 39 on Invasions of Privacy (Government Agencies) Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary, 89th Cong., 1st Sess., pt. 3, at 1158 (1965).

[22] See Brown, supra note 17, at 281-82; Lumbard, The Lawyers' Responsibility for Due Process and Law Enforcement, 12 Syracuse L. Rev. 431, 436 (1961); Comment, supra note 19, at 98.

[23] See Comment, Eavesdropping, Informers and the Right of Privacy: A Judicial Tightrope, 52 Cornell L.Q. 975, 976-80 (1967).

[24] 388 U.S. 41 (1967).

[25] 389 U.S. 347 (1967).

limited by statute. Section 605 of the Federal Communications Act of 1934[26] prohibits the interception and public divulgence of the contents of *any* wire communication or its interception for personal benefit. The Department of Justice has contended that this section requires both interception and divulgence to invoke the statute, therefore, taps for investigative purposes, not used as evidence, are legal.[27] The Court, however, has not accepted this interpretation.[28]

Other forms of electronic eavesdropping are not prohibited by statute and are subject only to the constitutional limitations imposed by judicial decisions. Until 1967 an exclusionary rule was applied only to electronic surveilliance accomplished by means of trespass of a constitutionally protected area.[29] Consent of one of the parties obviated the problem,[30] and interception without a trespass was permissible.[31] The Supreme Court's decisions in *Berger* and *Katz* changed the basic tenor of the law in this area. In *Berger*, the Court held unconstitutional a New York statute providing for the issuance of eavesdropping warrants and an investigation held thereunder, outlining the standards a "constitutional" state or federal eavesdropping statute must meet.[32] The Court held that authorization to eavesdrop be issued only upon probable cause to believe that a specific crime has been or is being committed; that the conversations to be seized be particularly described; that the authorization be of short duration; that the authorization terminate once the conversation sought is seized; that there be a "showing of exigency in order to avoid notice"; [33] and that there be a mandatory return on the warrant.

In *Katz*, the Court finally discarded the formalistic test based on a technical trespass of a constitutionally protected area and analyzed the problem as a general invasion of privacy question, although they were careful to disclaim any use of the fourth amendment to establish a more general constitutional right to privacy. The search in this case was held unconstitutional because the government agents:

> were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled during the conduct of the search itself to observe precise limits established in advance by a specific court order nor were they directed after the search had been completed to notify the authorizing magistrate in detail of all that had been seized.[34]

The Court, in holding that no eavesdrop could conceivably come within any of the exceptions to the rule requiring a search warrant, has defeated any argument that legal eavesdropping might be necessary without prior judicial authorization because of some last minute tip, at least in those cases to which the Court was addressing itself.[35]

The present state of federal administrative policy on electronic eavesdropping is definitive. Congressional hearings of the early 1960's disclosed widespread government agency use of electronic eavesdropping. Following this, President Johnson issued a directive ordering all federal agencies to cease wiretapping.[36] Finally, in 1967 Attorney General Ramsey Clark issued a memorandum essentially ordering the cessation of wiretapping and electronic eavesdropping without his authority. Clark's memorandum provided that:

---

[26] 47 U.S.C. § 605 (1964).

[27] See Katzenbach, An Approach to the Problems of Wiretapping, 32 F.R.D. 107 (1963). See also Swire, Eavesdropping and Electronic Surveillance: An Approach for a State Legislature, 4 Harve. J. Legis. 23 24-27 (1966).

[28] Orfield, Wiretapping in Federal Criminal Cases, 42 Texas L. Rev. 983, 992 (1964).

[29] E.g., Berger v. New York, 388 U.S. 41 (1967); Lopez v. United States, 373 U.S. 427 (1963); Silverman v. United States, 365 U.S. 505 (1961). See generally Gasque Wiretapping a History of Federal Legislation and Supreme Court Decisions, 15 S.C.L. Rev. 593 (1963).

[30] Osborn v. United States, 385 U.S. 323 (1966); Lopez v. United States, 373 U.S. 427 (1967); On Lee v. United States, 343 U.S. 747 (1952).

[31] E.g., Goldman v. United States, 316 U.S. 129 (1942); Olmstead v. United States, 277 U.S. 438 (1928).

[32] Berger v. New York, 388 U.S. 41 (1967). This article does not deal with the related problem of secret agents which differs with respect to overt deception, encouragement, and solicitation. For an excellent discussion of this problem see Note, Judicial Control of Secret Agents, 76 Yale L.J. 994 (1967).

[33] Berger v. New York, 388 U.S. 31 (1967).

[34] Katz v. United States, 389 U.S. 347, 356 (1967).

[35] Id. at 358 n.23.

[36] See Hearings on S. 928 Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary, 90th Cong., 1st Sess., pt. 1, at 33 (1967).

> It is essential that all agencies having any responsibility for law enforcement take steps to make certain that electronic and related devices designed to intercept, overhear, or record private verbal communications be subject to tight administrative control to assure that they will not be used in the manner in which it is illegal and that even legal use of such devices will be strictly controlled . . .
>
> Section 605 of the Communications Act . . . prohibits the interception and divulgence or use of telephone communications and is applicable to federal law enforcement agents . . .
>
> Interception by federal personnel of telephone conversations by any mechanical or electronic devices unless with the consent of one of the parties to the conversation is prohibited by presidential directive and this prohibition applies whether or not information which may be acquired through interception is intended to be used in any way or to be subsequently divulged outside the agency involved . . .
>
> . . . Any use of mechanical or electronic devices by federal personnel to overhear or record nontelephone conversations involving a violation of the Constitution or a statute is prohibited.
>
> . . . Agencies shall, except as provided . . . below obtain advance written approval from the Attorney General for any use of mechanical or electronic devices to overhear, record nontelephone conversations without the consent of all the parties to such conversations.[37]

The only exception to this thorough-going federal policy, which regularly goes unquestioned, is for "national security" cases. With respect to this exception the memorandum states:

> [T]he foregoing rules have been formulated with respect to all agency investigations other than investigations directly related to the protection of the national security. Special problems arising with respect to the use of devices of the type referred to herein in national security investigations shall continue to be taken up directly with the Attorney General in the light of existing stringent restrictions.[38]

To fully understand the consequences of this "national security" justification —which derives no basis from the language of section 605—and to understand the statute proposed herein, an intensive review of the congressional history and administrative practice concerning electronic eavesdropping during the past thirty years is necessary. Throughout this period the law remained unchanged; *all* wiretapping violated the absolute ban of section 605 of the Federal Communications Act of 1934, and *all* other electronic eavesdropping which resulted in a trespass of a constitutionally protected area was prohibited.

Prior to the 1940's the justification for wiretapping was based primarily upon domestic issues—the need to detect kidnappers, extortionists, and to curb the illegal activities of organized crime. After 1940 the rationale shifted, emphasizing international issues—the justification was the need to protect the "national security." This new rationale, advanced both within the executive branch and before Congress, presumably sought well-defined and limited grants of authority to protect the nation against foreign subversion.[39] In fact, as opposed to this rhetoric, the procedures were vaguely defined and the actual resort to illegal wiretapping was extensive. The role of the Department of Justice in this sphere was one of serious abuse; perhaps since the Department's concern was primarily with effective prosecution rather the protection of individual rights. The situation became complicated as section 605 was ignored and presidential directives were issued removing effective restraints on federal power and authority ostensibly for "national security" and hence political reasons.

The most important events which contributed to this changed rationale, derived from the political context, were World War II and the Cold War. World War II provided an event of specific and limited duration that was

---

[37] N.Y. Times, July 7, 1967, at col. 2-3.

[38] Id. col. 6.

[39] See, e.g., Letter from Attorney General Clark to President Truman, July 17, 1946, on file in Truman Library, Stephen Spelngarn Papers (executive branch rationale); N.Y. Times, Jan. 15, 1949, at 1, col. 8 (Justice Dep't rationale to Congress).

used to justify extensive wiretapping by federal agencies.[40] Far more significant with respect to more recent unauthorized wiretapping, however, was the nature and scope of the Cold War. The deterioration of United States-Soviet relations and the resultant concern over domestic subversive activites allegedly legitimized drastic new procedures. In 1947, a permanent loyalty program was instituted.[41] The formerly temporary wartime restrictions became an endemic part of American politics, redefining priorities and increasing concern over measures that presumed to protect the national security.

This changed political atmosphere is reflected most dramatically in the position adopted by the Department of Justice.[42] Prior to 1950, the Department sought to conceal its wiretapping activities, to deny in specific circumstances allegations that agents of the Federal Bureau of Investigation (FBI) had resorted to illegal wiretapping, or to deny that wiretapping was in violation of existing laws. After 1950, Department spokesmen openly admitted that wiretapping was an established practice and demanded that this action be legailized.[43] The sense of embarrassment and apology that characterized earlier reluctant admissions that FBI agents had wiretapped was not characteristic of the post-1950 period.[44]

A formal shift in rationale occurred in 1940 with a joint effort by the Justice Department and Congress to legalize wiretapping in "national defense" cases. Congressman Emanuel Celler (Democrat, New York) introduced a bill in 1940 which would have amended section 605 to permit the FBI to wiretap, subject to approval of the Attorney General. This law would have made the information so obtained admissible as evidence in cases involving interference or attempts to interfere with the national defense by sabotage, espionage, conspiracy, violation of the neutrality laws or "in any other manner." [45] The formal shift in Department rationale was expressed in a letter by Attorney General Jackson, dated May 31, 1940, to Congressman Celler affirming the need for legislation legalizing wiretapping.[46] Jackson wrote:

In a statement made by me to press on March 15, 1940, the following observations are found on this general subject:

> "In a limited class of cases, such as kidnapping, extortion, and racketeering, where the telephone is the usual means of conveying threats and information, it is the opinion of the present Attorney General as it was of Attorney General Mitchell that wiretapping should be authorized under some appropriate safeguard. Under the existing state of the law and decisions, this cannot be done unless the Congress sees fit to modify the existing statutes." [47]

The philosophy underlying the foregoing remarks, which were directed to the activities of the underworld, would seem applicable with even greater force to the activities of persons engaged in espionage, sabatotage, and other activities interfering with the national defense. This broad request to weaken section 605's absolute ban on wiretapping encountered studied opposition in 1940 from liberals concerned with the possible ramifications for civil liberties, the labor

---

[40] The outbreak of the war, even before U.S. involvement, had caused administration and congressional concern over subversion. The anti-national role of fascist and communist parties in Czechoslovakia, Austria, and France contributed to this sense of urgency; the war provided a specific time limit for effective action. For a discussion of the wartime loyalty program see E. Bontecou, The Federal Loyalty-Security Program 6-21 (1953). Congressional antipathy to wiretapping was reflected in the tone of the Hearings pursuant to S. Res. 224 on Investigation of Alleged Wiretapping Before a Subcomm. of the Senate Comm. on Interstate Commerce, 76th Cong., 3d Sess. (1940).

[41] The Federal Employees Loyalty Program was instituted by President Truman in March, 1947. See Exec. Order No. 9835, 3 C.F.R. 129 (Supp. 1947).

[42] N.Y. Times, April 1, 1949, at 48, col. 7; id., Dec. 1, 1949, at 28, col. 3; id., Feb. 2, 1950, at 14, col. 3; id., April 16, 1950, § 6 (Magazine), at 9; Justice Dep't Press Release, Jan. 8, 1950, on file in Justice Dep't Library.

[43] N.Y. Times, Nov. 18, 1953, at 20, col. 2; id., April 3, 1954, at 7, col. 1; id., April 7, 1954, at 20, col. 3; id., April 24, 1954, at 1, col. 7; id. at 12, col. 7; id., Feb. 25, 1955, at 1, col. 3; id. at 13, col. 4; id., March 24, 1955, at 22, col. 3; id., May 19, 1958, at 22, col. 3.

[44] N.Y. Times, Feb. 25, 1955, at 1, col. 3; id. at 13, col. 4; id., April 21, 1954, at 18, col. 1.

[45] H.R. Rep. No. 2574, 76th Cong., 3d Sess. (1940).

[46] Id. at 3.

[47] Id.

movement and political activism.[48] Because the United States was not then formally involved in World War II, and indeed the general public mood was one of opposition to formal involvement, the national defense argument carried less weight.

Simultaneously with this House effort, the Subcommittee of the Senate Committee on Interstate Commerce held formal hearings, from May 21, 1940 through February 15, 1941, to investigate previous wiretapping practices and to determine whether further legislative safeguards were needed.[49] These hearings reflected concern that despite the prohibitions of section 605 of the Federal Communications Act of 1934, government agencies had used wiretapping to investigate the political activities and beliefs of public employees and private citizens. The Senate Report expressed the Committee's concern that these abuses would be repeated and a fear that police agencies were unlikely to abide by prohibitions on wiretapping.[50]

These differing priorities and fears precluded congressional enactment of permissive wiretapping legislation. Resort to wiretapping was thereby stymied. Nonetheless, President Roosevelt did issue an executive directive permitting wiretapping in limited cases involving the "national defense." [51] The effect of this directive was to establish presidential responsibility for the use of illegal wiretapping. Surveillance was permitted based upon the premise that section 605 and Supreme Court decisions in *Nardone v. United States*,[52] and *Weiss v United States*,[53] only prohibited divulgence but not the actual interception. President Roosevelt, principally concerned with developments in Europe, however, sought to allow restricted use of illegal wiretapping. His directive of May 21, 1940 stipulated that:

> I have agreed with the broad purpose of the Supreme Court decision relating to wire-tapping in investigations. The Court is undoubtedly sound both in regard to the use of evidence secured over tapped wires in the prosecution of citizens in criminal cases; and it is also right in its opinion that under ordinary and normal circumstances wire-tapping by Government agents should not be carried out for the excellent reason that it is almost bound to lead to abuse of civil rights.
>
> However, I am convinced that the Supreme Court never intended any dictum in the particular case which it decided to apply to grave matters involving the defense of the nation.
>
> It is, of course, well known that certain other nations have been engaged in the organization of propaganda of so-called "fifth columns" in other countries and in preparation for sabotage, as well as in active sabotage.
>
> It is too late to do anything about it after sabotage, assassinations and "fifth column" activities are completed.
>
> You are, therefore, authorized and directed in such cases as you may approve, after investigations of the need in each case, to authorize the necessary investigating agents that they are at liberty to secure information by listening devices direct to the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies. *You are requested furthermore to limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens.*[54]

---

[48] For a general sense of this concern see Hearings pusruant to S. Res. 224 on Investigation of Alleged Wiretapping Before a Subcomm. of the Senate Comm. on Interstate Commerce, 76th Cong., 3d Sess. (1940). Of major concern was whether resort to wiretapping by federal, state, and local authorities had partisan or anti-union objectives. These concerns were directly expressed in the Committee Report in justifying the resolution that the 1940 hearings be held. S. Rep. No. 1304, 76th Cong., 3d Sess. (1940).

[49] See note 48 supra.

[50] S. Rep. No. 1304, 76th Cong., 3d Sess. (1940).

[51] Memorandum from President Roosevelt to Attorney General Jackson, May 21, 1940, on file in Truman Library, Stephen Speingarn Papers.

[52] 308 U.S. 338 (1939).

[53] 308 U.S. 321 (1939).

[54] Memorandum from President Roosevelt to Attorney General Jackson, May 21, 1940, on file in Truman Library, Stephen Speingarn Papers (emphasis added). The final sentence was subsequently deleted by Attorney General Clark when citing Roosevelt's directive as basic rationale for his suggested new directive.

The United States' entrance into World War II provided a setting different from that in 1940 which had prevented congressional enactment of legalized wiretapping. Accordingly, on April 23, 1942, Congressman Celler renewed his effort to secure a wiretapping bill.[55] His 1942 measure, in contrast to that of 1940, specifically provided that section 605 of the Federal Communications Act of 1934 would be waived in the "interest of prosecution of the war." [56] The report submitted to accompany this proposed bill stressed the need for wiretapping as a device for counter-espionage. Conceding the possible restrictions on individual rights, the report suggested that such fears were unwarranted since the use of wiretapping would be limited to the duration of the war and the activities restricted to necessary counter-espionage.[57] Congressman Celler's 1942 effort, as that of 1940, was unfruitful. Throughout the war illegal wiretapping was conducted pursuant solely to the restrictions and authority provided by President Roosevelt's directive and the information so obtained, although helpful for surveillance purposes, could not be used as evidence.

The FBI's use of wiretapping under this directive involved not only clear-cut security cases, such as the tapping of the telephones of the Japanese consulate in Hawaii,[58] but also extended to non-security cases presumably not covered by that directive, such as the tapping of Mrs. Franklin Roosevelt's Chicago hotel room by Army intelligence during World War II.[59] The termination of World War II brought into question the continued utilization of "illegal" wiretapping under the Roosevelt directive.

Attorney General Tom Clark, concerned over the deterioration of United States-Soviet relations, the prospect of Soviet espionage and the subversive role of the United States Communist Party, in 1946 secured President Truman's assent to a reaffirmation of Roosevelt's 1940 directive.[60] By quoting selectively from President Roosevelt's earlier directive—distorting the intent and scope of that directive—Clark secured President Truman's permission for an expanded authorization of wiretapping including a wider spectrum of "national security" cases and criminal activites. Clark's directive of July 17, 1946 stipulated that:

> Under date of May 21, 1940, President Franklin D. Roosevelt, in a memorandum addressed to Attorney General Jackson stated:
>
> "You are therefore authorized and directed in such cases as you may approve, after investigation of the need in each case to authorize the necessary investigating agents that they are at liberty to secure information by listening devices directed to the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies."
>
> This directive was followed by Attorneys General Jackson and Biddle, and is being currently followed in this Department. I consider it appropriate to bring the subject to your attention at this time.
>
> It seems to me in the present troubled period in international affairs, accompanied as it is by an increase in *subversive activities here at home*, it is as necessary as it was in 1940 to take the investigative measures referred to in President Roosevelt's memorandum. At the same time, the country is threatened by a very substantial increase in *crime*. While I am reluctant to suggest any use whatever of these special investigative measures in domestic cases, it seems imperative to use them in cases *vitally affecting the domestic security*, or where human life is in jeopardy.
>
> As so modified, I believe the outstanding directive should be continued in force. If you concur in this policy, I should appreciate it if you would so indicate at the foot of this letter.
>
> In my opinion, the measures proposed are within the authority of law, and I have in the files of the Department materials indicating to me that

---

[55] H.R. Rep. No. 2048, 77th Cong., 2d Sess. (1942).
[56] Id. at 1.
[57] Id. at 2.
[58] N.Y. Times, Nov. 14, 1945, at 3, col. 3; id., Feb. 14, 1946, at 18, col. 1.
[59] N.Y. Times, Nov. 1, 1965, at 1, col. 4.
[60] Letter from Attorney General Clark to President Truman, July 17, 1946, on file in Truman Library, Stephen Speingarn Papers (emphasis added). Not only had Clark deleted Roosevelt's qualifying sentence, but the national security concern of the Clark directive was broader and vaguer and could encompass surveillance of political and trade union activities.

my two most recent predecessors as Attorney General would concur in this view.[61]

Under this new directive, the scope of authorized "legal" wiretapping incorporated a broad range of activities. The provision "vitally affecting the domestic security, or where human life is in jeopardy" would include not only kidnapping but suspect political activities. In those limited cases where FBI resort to illegal wiretapping became public, this more general political aspect was fundamental. Reportedly, United Mine Worker's President John L. Lewis' phone was tapped and an FBI agent was apprehended allegedly installing the tap.[62] The phone of Edward Condon, Director of the Bureau of Standards, also had been tapped at various times from 1946 through 1949.[63]

In 1949, the Department of Justice instroduced a comprehensive internal security bill containing a section legalizaing wiretapping in "national security" cases.[64] Related to this legislative effort, and in the context of the 1949–50 trials of Judith Coplon, a former Justice Departmment employee, the wiretapping activities of the FBI came under critical focus and aroused great concern.[65] Arrested on charges of stealing Justice Department investigative secrets for a Soviet agent, Miss Coplon became a *cause celebre*. Interest in her case centered less on the criminal charge than on FBI investigative tactics and the subsequent disclosure that FBI agents had engaged in illegal wiretapping.[66] Attempting to undercut the reaction precipitated by these developments, FBI Director J. Edgar Hoover[67] and Attorney General Clark defended the Department's actions by relying on President Roosevelt's liberal credentials. Indeed, Clark claimed that resort to illegal wiretapping had not been concealed and had only occurred "in limited cases with the express approval in each individual instance of the Attorney General. There has been *no new policy or procedure* since the initial policy was stated by President Roosevelt and this has *continued* to be the Department's policy whenever the security of the nation is involved."[68] In January 1950, Clark's successor, Attorney General J. Howard McGrath, offered the same rationale for illegal wiretapping.[69] McGrath, again invoking President Roosevelt's directive and not

---

[61] Id.

[62] N.Y. Times, Oct. 6, 1948, at 25, col. 5.

[63] N.Y. Times, Dec. 16, 1949, at 20, col. 6.

[64] N.Y. Times, Jan. 15, 1949, at 1, col. 8. Owing to suspicions aroused by the Coplon case and more general concern over this specific request, Clark subsequently withdrew the request for legislation legalizing wiretapping. Id., April 1, 1949, at 48, col. 7.

[65] N.Y. Times, Dec. 1, 1949, at 28, col. 3; id., Dec. 16, 1949, at 20, col. 6; id., Jan. 1, 1950, at 12, col. 1; id., Jan. 12, 1950, at 9, col. 3; id., Feb. 2, 1950, at 14, col. 3; id., Feb. 2, 1950, at 14, col. 3; id., Nov. 3, 1950, at 24, col. 2.

[66] Justice Dep't concern over the reaction is reflected in press releases by Attorneys General Clark and McGrath. See Justice Dep't Press Release, March 31, 1949, on file in Justice Dep't Library; id., Jan. 8, 1950, on file in Justice Dep't Library. During the trials it was disclosed that F.B.I. agents had tapped Miss Coplon's phone, that the taps had occurred before and after her arrest and included privileged conversations between Miss Coplon and her attorneys. N.Y. Times, Dec. 1, 1949, at 28, col. 3; id., Dec. 16, 1949, at 20, col. 6; id., Jan. 1, 1950, at 12, col. 1; that Mr. Gubitchev's phone (the Soviet agent involved) had been tapped with the prospect that this had involved widespread tapping of the phones of other United Nations employees. N.Y. Times, Dec. 1, 1949, at 28, col. 3; id., Dec. 16, 1949, at 20, col. 6; id., Jan. 12, 1950, at 9, col. 3; that F.B.I. agents in pretrial testimony had denied having tapped Miss Coplon's phone and subsequently admitted wiretapping when the defense presented tapes of those taps. N.Y. Times, Feb. 2, 1950, at 14, col. 3; and that local F.B.I. agents had destroyed wiretap records immediately prior to trial, N.Y. Times, Nov. 3, 1950, at 24, col. 2.

These disclosures created a furor since they involved not only evidence of illegal F.B.I. wiretapping, but also definite violations of individual rights. Most dramatic were the disclosures concerning taps of Miss Coplon's privileged conversations with her lawyers, the perjured testimony of F.B.I. agents and their seeming effort to conceal their activities by destroying the wiretap records. This was coupled with Department of Justice efforts to prevent the defense attorneys from publicizing the F.B.I. records that Miss Coplon was accused of stealing, records which disclosed F.B.I. surveillance of the personal and political association of prominent liberals both inside (Edward Condon, David Niles) and outside the Administration (Frederick March, Edward G. Robinson). N.Y. Times, June 2, 1949, at 3, col. 7; id., June 3, 1949, at 2, col. 2; id., June 4, 1949, at 2, col. 3; id., June 8, 1949, at 1, col. 2; id., June 9, 1949, at 1, col. 8; id., June 10, 1949, at 10, col. 3; id., June 11, 1949, at 6, col. 1; id., June 12, 1949, at 1, col. 2; id., June 16, 1949, at 15, col. 5; id., Dec. 16, 1949, at 20, col. 6. See also Coplon v. United States, 191 F.2d 749 (D.C. Cir. 1951), cert. denied, 342 U.S. 926 (1952); United States v. Coplon, 185 F.2d 629 (2d Cir. 1950), cert. denied, 342 U.S. 920 (1952).

[67] N.Y. Times, April 16, 1950, § 6 (Magazine), at 9.

[68] Justice Dep't Press Release, March 31, 1949, on file in Justice Dep't Library (emphasis added).

[69] Justice Dep't Press Release, Jan. 8, 1950, on file in Justice Dep't Library.

President Truman's of 1946, asserted that the FBI's resort to wiretapping had been based on the earlier Roosevelt directive. McGrath specifically affirmed that there had been no new policy or procdure concerning wiretapping since President Roosevelt.[70]

A complex of events, particularly the outbreak of the Korean War and an internal security phobia that dominated American thought, changed the climate in which the resort to wiretapping came to be discussed in Congress. The *Coplon* case led to a reassessment of the rationale for restrictions against the use of evidence secured through wiretapping. The central concern of the Congress no longer centered on possible dangers that the resort to wiretapping posed for constitutional rights, but on whether the prohibition of section 605 of the Federal Communications Act of 1934 should be continued. The implication was that this prohibition possibly endangered, or at least compromised, the "national security." In 1951, 1953, 1954, 1958 and 1959, specific legislation was introduced and hearings held concerning legalization of wiretapping in "national security" cases.[71] The Department of Justice and the various military agencies emphasized the necessity of wiretapping, and it was asserted that the Act prohibited only the divulgence of information secured through wiretapping.[72] Moreover, the Department of Justice's formerly apologetic attitude over the resort to illegal wiretapping was tacitly rejected by Attorney General Brownell who forthrightly admitted in 1954 that the number of wiretaps in operation reached as high as 200 at any one time. Brownell cited these figures as evidence of Department vigilance.[73]

The proposed legislation and hearings conducted pursuant to these post-1950 recommendations highlight this shift in priorities and concerns. The legality of FBI resort to wiretapping went unquestioned. At issue were these questions: what procedures or guildelines should be established; what actions would be legalized; and where should the final authority for approving specific wiretapping be vested, in the Attorney General or in federal judges?[74] Moreover, in hearings held in 1953, Congressman Celler specifically affirmed that the purpose of the hearings was not to investigate incidents of illegal wiretapping, but rather to establish the provisions for the legal use of evidence secured through wiretapping.[75] The committee report published subsequent to these hearings stipulated that the resort to wiretapping was not a constitutional but a legislative question.[76] The report affirmed that section 605 of the Federal Communications Act had imposed definite restrictions on the use of wiretapping information as evidence. It criticized this restriction as harmful to the "national security" and recommended the enactment of legalized wiretapping legislation in cases generally affecting the "national security."[77]

---

[70] Id.

[71] N.Y. Times, Nov. 18, 1953, at 20, col. 2; id., April 3, 1954, at 7, col. 1; id., April 24, 1954, at 1, col. 7; id., Feb. 25, 1955, at 1, col. 3; id. at 13, col. 4; id., March 24, 1955, at 22, col. 3; id., May 15, 1958, at 59, col. 3; id., Dec. 16, 1959, at 34, col. 1. In 1965, it was revealed that I.R.S. agents had used wiretaps in the federal government's attack on organized crime in Pittsburgh and that F.B.I. agents had tapped the phones of businessmen in private homes and apartments in connection with investigations involving suspicions of criminal activities. N.Y. Times, July 16, 1965, at 6, col. 3; id., Oct. 24, 1965, at 50, col. 1.

[72] N.Y. Times, Nov. 18, 1953, at 20, col. 2; id., April 3, 1954, at 7, col. 1; id., April 21, 1954, at 18, col. 1; id., April 24, 1954, at 1, col. 7; id. at 12, col. 7; id., Feb. 25, 1955, at 1, col. 3; id. at 13, col. 4; id., March 24, 1955, at 22, col. 3; id., May 15, 1958, at 59, col. 3; id; Dec. 16, 1959, at 34, col. 1; H.R. Rep. No. 1461, 83d Cong., 2d Sess. 3 (1954); Hearings on Wiretapping for National Security Before Subcomm. No. 3 of the House Comm. on the Judiciary, 83d Cong., 1st Sess. (1953); Hearings on Wiretapping Before Subcomm. No. 5 of the House Comm. on the Judiciary, 84th Cong., 1st Sess. (1955).

[73] N.Y. Times, April 21, 1954, at 18, col. 1. In contrast to this admission by Brownell, in 1931 F.B.I. Director Hoover had emphatically denied that wiretapping was permitted. Hoover then averred that "we have a very definite rule in the bureau that any employee engaged in wiretapping will be dismissed from the bureau." Hearings on Wiretapping in Law Enforcement Before the House Comm. on Expenditures in the Executive Departments, 71st Cong., 3d Sess. 26 (1930).

[74] H.R. Rep. No. 1461, 83d Cong., 2d Sess. (1954); Hearings on Wiretapping for National Security Before Subcomm. No. 3 of the House Comm. on the Judiciary, 83d Cong., 1st Sess. (1953); Hearings on Wiretapping Before Subcomm. No. 5 of the House Comm. on the Judiciary, 84th Cong., 1st Sess. (1955).

[75] Hearings on Wiretapping for National Security Before Subcomm. No. 3 of the House Comm. on the Judiciary, 83d Cong., 1st Sess. 16-17 (1953).

[76] H.R. Rep. No. 1461, 83d Cong., 2d Sess. 1-3 (1954).

[77] Id. at 4.

During committee hearings in 1953, no effort was made to define the term "national security" with any precision. The language of one of the proposed bills, that of Congressman Celler, delineated national security as encompassing "treason, sabotage, espionage, sedition, sedition conspiracy, violation of the neutrality laws, violation of the Act of requiring the registration of agents of foreign principals . . . , violation of the Act requiring the registration of organizations carrying on certain activities within the United States . . . [and] violation of the Atomic Energy Act of 1946 . . . ." [78]

Neither these bills nor the terms under reference clearly defined or delineated what constituted subversive or "certain" activities. Nor did the committee in its hearings or report secure a clear, defined limit. A broad standard was implicitly accepted—tacitly the Department of Justice would be accorded considerable leeway in surveillance of actions or activities that affected the "national security."

The language used in 1954 to define "national security"—"treason, sabotage, espionage, sedition, conspiracy, violation of Chapter 115 of Title 18 of the United States Code, violation of the Internal Security Act of 1950 . . . , violations of the Atomic Energy Act of 1948 . . . and conspiracies involving any of the foregoing," [79] repeated this process. With the exception of Congressman Keating's 1958 bill,[80] the same language was used throughout the latter 1950's when similar bills were introduced.[81] Despite the changed rationale and focus these various legislative efforts failed. Congress did not enact specific wiretapping legislation although the momentum for passage had increased and a reluctance to prohibit the use of wiretapping on alleged "national security" grounds had emerged.

With the advent of the 1960's a change in emphasis, although not in rationale, took place. As an omen of this change Congressman Celler's 1959 bill included a clause which would have authorized wiretapping in kidnapping cases.[82] As a result of the investigative disclosures of the Kefauver [83] and McClellan [84] Committees, the primary concern shifted from "national security" to organized crime. Bills introduced in 1961 and 1962 retained the definition of "national security" as "any offense punishable by death or imprisonment for more than one year under chapter 37, 105, or 115 of title 18 of United States Code, Sections 224–227 inclusive of the Atomic Energy Act of 1954 . . . , as amended, or conspiracy to commit any such offense." [85] But to this was added authorization to wiretap for any offense involving murder, kidnapping or extortion under title 18 of the United States Code any offense under sections 201, 202, 1084, or 1952 of title 18 of the United States Code any offense under any law of the United States involving the manufacturing of, importation, receiving, concealment, buying, selling or otherwise dealing in narcotic drugs, marihuana or any conspiracy to commit any of the foregoing offenses.[86]

During the period of the late 1950's and early 1960's use of illegal electronic eavesdropping by the executive branch continued. In 1959 Attorney General William P. Rogers told the Senate committee investigating the use of wiretapping that the FBI had 74 telephone taps all of which were for "national secu-

---

[78] Hearings on Wiretapping for National Security Before Subcomm. No. 3 of the House Comm. on the Judiciary, 83d Cong., 1st Sess. 1 (1953). Similar definitions were established in other bills considered by the Committee. Id. at 2-4. The most general of these bills simply refered to but never defined, "national security." Id. at 4.

[79] Hearings pursuant to S. Res. 62 on Wiretapping, Eavesdropping, and the Bill of Rights Before the Subcomm. on Contstitutional Rights of the Senate Comm. on the Judiciary, 86th Cong., 1st Sess., pt. 3, at 1014 (1959).

[80] Id. at 1021.

[81] Congressman Celler's 1959 bill defined "national security" as:
one or more of the crimes punishable under Chapter 7 (dealing with espionage), . . . Chapter 105 (dealing with sabotage), or Chapter 115 (dealing with treason, sedition, and subversive activities) of this title, or section 10 of the Atomic Energy Act of 1946 . . . , as amended, or a conspiracy to commit any such crimes.
Id. at 1027.

[82] Id.

[83] See S. Rep. No. 307, 82d Cong., 1st Sess. (1951).

[84] See Hearings Before the Senate Select Comm. on Improper Activities in the Labor or Management Field, 85th Cong., 1st & 2d Sess. (1957-58); id., 86th Cong., 1st Sess. (1959).

[85] Hearings on S. 2813 & S. 1495 Before the Senate Comm. on the Judiciary, 87th Cong., 2d Sess. 2 (1962).

[86] Id. at 3.

rity" cases.[87] At the 1961 Senate committee hearings Assistant Attorney General Miller testified that the FBI had 85 wiretaps at that time, all authorized on "national security" grounds.[88] Hearings in 1965 disclosed widespread use of wiretapping and electronic eavesdropping by many federal agencies especially by the Internal Revenue Service.[89] As a result the Justice Department was forced to admit in more than thirty cases that some of the evidence was possibly tainted resultiing from illegal wiretapping or electronic eavesdropping.[90] Among these were *Schipani v. United States* [91] and *Black v. United States* [92] In a 1966 memorandum to the Supreme Court in the *Black* case, then Solicitor General Thurgood Marshall wrote:

> [U]nder departmental practice in effect for a period of years prior to 1963 and continuing into 1965 the director of the Federal Bureau of Investigation was given authority to approve the installation of devices such as that in question for intelligence (and not evidentiary) purposes when required in the interest of internal security or national safety including organized crime, kidnapping and matters wherein human life be at stake. Acting on the basis of the aforementioned departmental authorizations the director approved installation of the device involved in the instant case.[93]

Thus, the "national security" exception was expanded to include organized crime cases in practice if not in theory.

In 1967 another bill [94] was introduced in the Congress and further hearings were held.[95] This bill prohibited the *interception* or the divulgence of any wire communication or th use of electronic eavesdropping devices sold in interstate commerce. The "national security" exception was continued, but in different language:

> [N]othing contained in this chapter or in section 605 of the CommunicationsAct of 1934 . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power or any other serious threat to the security to the United States or to protect national security information against foreign intelligence activity.[96]

During the hearings Attorney General Ramsey Clark admitted that the Department of Justice presently had approximately 38 wiretaps "in cases directly affecting the national security." [97] He said: "[t]here is no other wiretapping or other electronic surveillance engaged in by the Department of Justice." [98] He also specifically refused to interpret the language "any other serious threat to the security of the United States" as including organized crime cases.[99] This legislation also made no progress in Congress.

---

[87] Hearings pursuant to S. Res. 62 on Wiretapping, Eavesdropping, and the Bill of Rights Before The Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary, 86th Cong., 1st Sess., pt. 5, at 1481-82 (1959).

[88] Hearings on S. 1086 on Wiretapping and Eavesdropping Legislation Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary, 87th Cong., 1st Sess. 363 (1961).

[89] Hearings pursuant to S. Res. 39 on Invasions of Privacy (Government Agencies) Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary, 89th Cong., 1st Sess. (1965).

[90] N.Y. Times, Jan. 30, 1968, at 24, col. 1. The indications from Justice Department sources were that as a result of the Supreme Court's action in Kolod v. United States, 390 U.S. 136 (1968) (per curiam), about twice as many more such instances would be revealed. The Court in that decision rejected the Justice Department's position: that the department would first decide whether the eavesdropping was arguably relevant to any of the evidence for the prosecution. The Court held that this determination must be made by the district court after full disclosure by the government.

[91] 385 U.S. 372 (1966).

[92] 385 U.S. 26 (1966).

[93] Supplemental Memorandum for the United States to the U.S. Supreme Court in Hearings on S. 928 on Right of Privacy Act of 1967 Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary, 90th Cong., 1st Sess., pt. 1, at 34 (1967).

[94] S. 928, 90th Cong., 1st Sess. (1967).

[95] Hearings on S. 928 Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary, 90th Cong., 1st Sess. (1967).

[96] Id., pt. 1, at 3.

[97] Id. at 56.

[98] Id.

[99] In answer to a question by Senator Long as to whether, under the Attorney General's interpretation, the language "any other serious threat to the security of the United States" could be extended to organized crime cases and other similar criminal cases, the Attorney General answered: "We are speaking only of matters that directly effect the national security and are a threat to the Nation. This bill would, therefore, prohibit use of wiretapping for investigation of gambling, numbers, prostitution and such things as that." Id. at 51.

From this historical review, a somewhat circular pattern in the development of the legislative proposals becomes apparent. The first, and only successful, proposal was the blanket prohibition of section 605 of the Federal Communications Act of 1934. The next attempts were in terms of an undefined "national security" exception. Then followed statutes which were more specific being written in terms of violation of federal statutes—first "national security" statutes and later certain criminal statutes and conspiracy to commit violations of these statutes. Finally, there is the present proposal again involving a more or less undefinable "national security" exception.

III

A PROPOSAL

This historical review demonstrates the ease of administrative extensions in the face of the present blanket prohibition. Our conclusion is that there is a need for specific legislation which incorporates into its definitions specified violations and conspiracies to commit those violations. In spite of the Attorney General's reassurance, the authors remain concerned that subsequent administrations could extend the language, "any other serious threat to the security of the United States," to situations involving internal rather than external threats—such internal threats as organized crime, the black power movement [100] and the peace movement. We believe that wiretapping and other electronic eavesdropping are extreme police techniques and should be permitted only within strictly limited situations. Since there seems to be universal acceptance of the "national security" exception, we believe that it should be limited to threats mounted from a foreign source. Thus, in our proposed authorization for national security investigations we have included only those specific sections dealing directly with crimes involving foreign governments and have excluded any sections that in any conceivable way might be used to justify eavesdropping against internal political organizations.

Because of the great national concern with organized crime we propose an optional exception of an experimental nature authorizing wiretapping and electronic eavesdropping in certain cases of organized crime. An attempt has been made to limit the authorization to crimes committed primarily by organized syndicates, with the full knowledge that organized crime is involved in many other kinds of activities,[101] because we believe that the need of the police for extraordinary methods to combat *unorganized* crime has not been demonstrated to sufficiently outweigh the constitutional objections to electronic eavesdropping. Finally, in order to comport with the constitutional procedural requirements for eavesdropping warrants,[102] and in line with the *Katz* case for the organized crime section, and in spite of its ambiguity on national security,[103] we require a procedural protection of approval by the Attorney General and the issuance of a wiretap or eavesdropping warrant by an impartial federal magistrate.

We therefore submit the following amendment to the 1967 bill. Substitute Section 2514A, National Security.

> Subject to the provisions of Section 2514C, authorization may be issued for the use of wire interception and eavesdripping devices in cases involving violations of United States Code, title 18, chapter 37 (espionage), sec-

---

[100] Militant black power leaders are certain that their phones are tapped by the F.B.I. See, e.g., Malcolm X, Autobiography 257 (1965); Wills, The Second Civil War, Esquire, March 1968, at 144. These beliefs are supported by the Justice Department's recent implicit disclosure that it had extensively bugged and tapped the W.E. DuBois Clubs. N.Y. Times, March 20, 1968, at 18, col. 4.

[101] The 1965 Presidential Commission described the activities of organized crime: The core of organized crime activity is the supplying of illegal goods and services—gambling, loan sharking, narcotics, and other forms of vice—to countless numbers of citizen customers. But organized crime is also extensively and deeply involved in legitimate business and in labor unions. Here it employs illegitimate methods—monopolization, terrorism, extortion, tax evasion—to drive out or control lawful ownership and leadership and to exact illegal profits from the public. And to carry on its many activities secure from governmental interference, organized crime corrupts public officials. President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society 187 (1967). See also Hundley, The Nature of Interstate Organized Crime and Problems in Law Enforcement, 39 Notre Dame Law. 627 (1963).

[102] See p. 750 supra.

[103] Katz v. United States, 389 U.S. 347, 358, n.23 (1967).

tions 792, 793, 794, 795, 796, or 797; or chapter 105 (sabotage), sections 2153, 2154, 2155, or 2156; or chapter 115 (treason and sedition), sections 2381, 2382, 2383, 2384, 2388, 2389, or 2390; or conspiracy to commit any of the above except section 2384.

Section 2514B, Organized Crime.

(a) Subject to the provisions of section 2514C, authorization may be issued for the use of wire interception and eavesdropping devices in cases involving violation of United States Code, title 18, sections 201 (bribery), 224 (sports bribery), 1084 (transmission of gambling information), or 1953 (racketeering); or any offense involving bankruptcy fraud or the importation of narcotics, or any conspiracy to commit any of the above.

(b) This section shall terminate automatically after five years after the passage of this act.

Section 2514C, Judicial Order.

(a) Every application for judicial authorization of the use of wire interception and eavesdropping devices shall contain: (1) a statement of approval of the application by the Attorney General of the United States; (2) a full and complete statement of the facts and circumstances relied upon by the applicant; (3) a showing of special need for the authorization; and (4) a complete statement of facts concerning all previous applications made for authorization under this statute involving the same communication facilities or places, or involving any person named in the application for having committed, or committing the same offense.

(b) A federal judge may issue an appropriate warrant if: (1) he has probable cause to believe that an offense specified in section 2514A or 2514B has been, is being, or is about to be, committed at the place at which the eavesdropping device is to be used or the conversation is to be intercepted by wire;[104] and (2) he believes that there is a special need to authorize the interception.

(c) Every order authorizing the use of wire interception or eavesdropping devices shall specify: (1) the findings of the judge pursuant to subsection (b) of this section; (2) the nature and location of the communications facilities as to which, or the place where, leave to intercept is granted; (3) a specific description of the conversation(s) to be intercepted and the persons under surveillance; (4) the offense about which information is to be sought; (5) the period of time for which such interception is authorized; and (6) the date and place at which the warrant is to be returned and the report of the results is to be made.

(d) No extensions of any warrant issued hereunder may be granted without complete review according to subsection (b).

ADDENDUM

After this article was written Congress passed and the President signed the Omnibus Crime Control and Safe Streets Act of 1968.[105] This Act permits judicial authorization of electronic surveillance by federal, state and local authorities in a variety of situations. It contains a two part authorization of electronic eavesdropping in "national security" cases. Under section 2511(3) the President retains his "constitutional power" to take necessary action to prevent "actual or potential attack or other hostile acts" by a foreign power, and "to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government." Under section 2516(1)(a) specific violations of comprehensive chapters of the United States Code are

[104] The usual problem of defining probable cause remains. The authors believe that this problem is best resolved on a case by case basis. A standard definition is that of Mr. Justice Douglas: "probable cause exists if the facts and circumstances known to the officer warrant a prudent man in believing that the offense has been committed." Henry v. United States, 361 U.S. 98, 102 (1959). See also Draper v. United States, 358 U.S. 307 (1959); Carroll v. United States, 267 U.S. 132 (1925). Perhaps under the unusual circumstances of the cases which will be candidates for the use of electronic eavesdropping, it might be necessary to adopt a standard more akin to that of "reasonable suspicion" which has been used in stop and frisk legislation. Cf. 74 Yale L.J. 942. 952 (1965). The stop and frisk type of approach has also been adopted in allowing a warrant to issue for crimes "about to be committed" in order to permit some degree of flexibility in the use of electronic eavesdropping devices.

[105] Pub. L. No. 90-351 (June 19, 1968).

enumerated as cases in which electronic eavesdropping may be authorized. This subsection, and the other parts of the section which attempt to deal with organized crime on both state and federal levels, is similar to the proposal of the President's Commission on Law Enforcement and Administration of Justice although it is somewhat broader and includes, under the "national security" exception, chapter 102 relating to riots. In addition, under the judicial procedure for the issuance of warrants established by section 2518, unauthorized electronic surveillance may proceed for a forty-eight hour period in "emergency situations." The authors believe that all these sections are overly broad, far exceeding what is both necessary and proper to combat espionage and organized crime. We are deeply concerned that the prime target of the "national security" provisions will be internal political organizations—presently the peace and black power movements. The sections attempting to deal with organized crime include several crimes which, while also committed by the Cosa Nostra, are predominantly committed by unorganized criminal elements. Finally, we have grave doubts about the necessity for and constitutionality of the "emergency situation" authorization of section 2518(7).[106]

Investigating The FBI—A Tough, Fair Look At The Powerful Bureau; Its Present And Its Future

ELECTRONIC SURVEILLANCE

(By Victor Navasky and Nathan Lewin)

I: The Omnibus Crime Act

It is ironic that Ramsey Clark, the first Attorney General in more than thirty years who did not ask Congress to legalize wiretapping, was presented with the Omnibus Crime Control and Safe Streets Act of 1968, which legalized both wiretaps and bugs. The argument of his predecessor Attorneys General was, in part, that since the FBI already engaged in wiretapping at the margins of the law (especially in the national security area), it would be better if such tapping were brought under explicit statutory control. So Title III of the 1968 act, with few exceptions, authorizes wiretaps and eavesdrops only on judicial warrant and with specified inventory and reporting conditions.

Attorney General Clark, who opposed electronic surveillance on principle and also believed it an inefficient law-enforcement instrument, declined to act under the provisions of the new law, but his successor, John Mitchell, enthusiastically moved to implement the new tapping and bugging authority.

One year's experience under the act is analyzed below. Here it is sufficient to note that despite the so-called legalization of tapping and bugging, the Nixon administration's actions are as dangerous and disingenuous as those of any preceding administration in this dark corner of law enforcement.

In April, 1971, President Nixon told the annual convention of the American Society of Newspaper Editors: "Now in the two years that we have been in office—now get this number—the total number of taps for national security purposes by the FBI, and I know because I look not at the information but at the decisions that are made—the total number of taps is less, has been less, than 50 a year."

But one month earlier, Assistant Attorney General Mardian wrote the Chairman of the Administrative Practices Subcommittee of the U. S. Senate that a total of ninety-seven warrantless telephone taps were operated in 1970—almost double the President's figure and almost triple the figure the Solicitor General mentioned in a brief filed with the U. S. Supreme Court in September, 1970, when he said only thirty-six warrantless telephone surveillances were operated in 1970.

Moreover, as Senator Edward Kennedy has observed, "the repeated references by Government officials to the limited number of warrentless devices ignore the far more significant question of the duration and total usage of these devices. I am extremely concerned by the fact that in 1970 there were from 3.4 to 9.6 times as many days of federal listening on warrantless devices as there were devices installed under judicial authorization."

---

[106] See pp. 754-55 supra.

As the Chairman concluded in a letter to the members of the Administrative Practices Subcommittee, contrary to recurring claims, by "informed sources" that federal electronic surveillance is shrinking, a study of correspondence with the U. S. Department of Justice and related public materials suggest that:

1. The number of federal wiretapping and bugging devices installed without court authorization is substantially greater than the executive branch has led the public to believe.

2. The average duration of such devices is many times longer than the average duration of court-approved devices.

3. As a result, the total amount of federal electronic eavesdropping without court permission far exceeds the eavesdropping with judicial approval.

4. There is strong reason to doubt the validity of the repeated public assurances by the Justice Department that it fully complies with the 1968 congressional standards before installing any tap or bug without a court order.

5. Despite the department's assertions to the contrary, there is an absence of well-defined procedures which would promote compliance with the statutory standards and permit meaningful congressional scrutiny of this extraordinary executive activity.

When J. Edgar Hoover appeared before Congressman Rooney's subcommittee in 1970 and 1971, he also testified to the number and type of electronic surveillances then maintained by the FBI. He had been doing the same thing for many years, but these were the first two years that the activity was supposed to be regulated by a specific federal law. Examination of his testimony also suggests that the safeguards of the new law are not enough.

Hoover's testimony implied that the total number of wiretaps and bugs was small and carefully limited—thirty-six and thirty-three in the national security field at the time of each respective appearance, and four and fourteen in the organized crime field. (Mr. Hoover was accused of turning off taps the day before he testified—and denied the accusation. But it would be consistent with the FBI's fetish for statistics for him to have chosen the date of his testimony with an eye to reduced tap figures.) Beyond that, there are three reasons why it is difficult to take Hoover's testimony (and other official estimates) at face value.

For one thing, the figures do not reflect the FBI's access to non-federal wiretaps and bugs. But as one recently retired Justice Department official told us, not only do agents have access to state and local electronic eavesdropping, but: "When I was there agents routinely inspired bugs and taps by others. They'd go to state and local police agencies and say, look, do us a favor. The local guys would get the information and there'd be nothing in the FBI files to indicate where it came from. It's a loophole, like the tax laws. They's use the loophole."

In 1970, in addition to the national security surveillance referred to in Hoover's testimony, the federal government got court warrants for 180 electronic surveillances and state and non-federal officials got warrants for 403.

Second, Mr. Hoover's testimony itself is incomplete even for the internal security area he purports to cover.

Since his 1968 testimony before Rooney's subcommittee (in support of the 1968 budget), Mr. Hoover framed his reports in terms of the number of wiretaps "in Bureau cases." This leaves open the possibility (indeed informed sources within the department indicate it is a fact) that although he has neglected to mention it to Congress, Mr. Hoover is not referring to all of the taps in which the Bureau is involved. (1) He may be omitting the long-term embassy taps which were put on in the first place—some as long ago as during World War II—not at the instigation of the FBI, but of other agencies, such as the State Department, but which the FBI services. (2) He is omitting all of the taps requested by foreign intelligence agencies such as the CIA, which are not permitted to tap domestically yet have domestic intelligence needs. The FBI handles those taps and passes on the information (which it also absorbs). (3) He is omitting the interception of teletype messages.

Third, there is the issue of unauthorized taps and bugs. Former agent William Turner is quite insistent that the "suicide tap"—wherein an agent, knowing that if he is caught he will be dismissed, nevertheless, under the pressure to produce, conducts illegal, unauthorized surveillance on an ad hoc basis. Most authorities on the FBI find stories of hit-and-run taps difficult to credit,

since "Mr. Hoover runs a tight ship," and "Why should an agent risk it?" Nevertheless, Turner, who attended the FBI's sound school in Washington, D.C., and monitored Bureau taps for a year and a half in the Bay area, points out, "All I know is that I did it and the term 'suicide tap' is a common term. You hear it whenever agents gather."

Turner adds, "My impression was that at least in the internal security area they had a pretty cavalier attitude. The idea was that our job was to protect the security of this country; that the Federal Communications Act was really meant for telephone companies anyway. They told you never to take your credentials when you do a *black bag job* [surreptitious entry]. They taught lock-picking at sound school. There was a procedure whereby a fellow agent would go over to the local police and hang around in case a burglary were reported in the house you were breaking into. Then he would tell the police what was happening and they would leave you alone."

It is, of course, impossible to tell how extensive such unauthorized tapping and bugging is. But once information from them gets into the FBI files, it is attributed to anonymous confidential informants and nobody is any the wiser.

Yet another problem in assessing the real quantity of electronic surveillance to which the FBI has access was pointed up by Ramsey Clark. He told a federal judge in Harrisburg, in connection with the Berrigan case, that false reports by FBI agents on their electronic surveillance activities caused the Justice Department "deep embarrassement" many times while he was Attotney General. "Often we would go into court and say there had been no electronic surveillance and then we would find we had been wrong."

Clark said that the government's response to the Berrigan defense motion for disclosure of all evidence by eavesdropping—that there was no evidence of surveillance except the overhearing of Sister Elizabeth McAlister—"is equivocal and amounts to a refusal to search theire records."

"I served in the Department of Justice for a good many years. Often you could not find out what was going on . . . frequently agents lost the facts," Clark said. One can argue that things have changed since then. Clark himself instituted elaborate reporting forms, and then there are the reporting requirements of the 1968 law. But there is really no way of knowing the effect of either.

A further problem in detecting the amount of electronic surveillance—authorized or otherwise—is that the issue never arises until a defendant in a particular case raises it, or until the government moves toward prosecution. One U.S. attorney recalls: "We were going to indict a lawyer in Florida in a fraud case. It was around August, 1967, and the SAC in charge came down to see me and asked could I hold up the indictment. He showed me a wire he got from the Bureau telling him that the lawyer's office had been bugged around 1963 in connection with Las Vegas skimming. Then I asked them to let me know what it showed. It turned out that this lawyer had had conversations with Hoffa, Bobby Baker, you name it. I finally thought they did this to make it as difficult as possible for me to indict because they didn't want the bug discovered. And they *did* scare me. I didn't bring the case. They had overheard about twenty top figures. We found out from an agent that the bug was installed by illegal trespass. It was *totally* unrelated to our case but we didn't want to go through all of that publicity and crap. I just didn't want to be in the position of justifying what the Bureau had done, and you always wonder, were they really telling you everything?"

Finally, there is the problem of translating what the public is told into what is really going on. As Professor Herman Schwartz of the law faculty at the State University of New York at Buffalo has shown, when the public is told that there were only 302 court-ordered electronic surveillances in 1969, it is not told this means 31,436 people were overheard in 173,711 conversations, not counting all those overheard without a court order.

The wiretapping provisions of the Omnibus Crime Act of 1968 require judges and prosecutors to file reports with the Administrative Office of the U.S. courts on each court-ordered wiretap or eavesdrop. Section 2519 of Title 18 specifies that the judge's report must cite the suspected offense, the kind of eavesdrop, its duration and the identity of the government official making the application. The prosecutor's report must specify, in addition, "the frequency of incriminating communications intercpted," and the frequency of "other communications intercepted," the approximate number of persons overheard, the cost of the

interceptions and the number of arrests, trials and convictions arising out of the interceptions.

The report for the 1970 calendar year issued by the Administrative Office of the U.S. courts covers all orders—federal and local—issued under the 1968 act. Its federal section, however, contains some interesting statistics.

1. A total of 183 federal eavesdrops were authorized by court order, and 180 were installed (three were abandoned after a court order was obtained). Every one was applied for by the assistant attorney general in charge of the Criminal Division.

2. Approximately two thirds of the 183 surveillances were for gambling and bookmaking charges, and drugs and "extortionate credit transactions"—not traditional "extortion" but what is known as "loan-sharking"—covered all but five of the remainder (these were broken down to two "robbery," two "stolen property" and one "forgery and counterfeiting").

What these figures plainly demonstrate is that the FBI, with the acquiescence and consent of the Justice Department, has seized all the benefits it can from the 1968 act without assuming any of its burdens. Having claimed for almost thirty years that it needed authority to tap telephones for espionage, sabotage, extortion and kidnapping cases, it has not found the need to take a single case of that kind before a federal judge for a wiretap order. Instead, it has channeled all cases coming within the jurisdiction of the Internal Security Division and Assistant Attorney General Mardian into the "national security" category which it said the act excepted from requiring a warrant, and has continued its pre-act practice of tapping and bugging in these situations without a warrant.

This is inconsistent with the representations made by the Department of Justice to the Supreme Court in the case testing the legality of warrantless electronic surveillances in national security investigations. In his brief, the solicitor general argued that to permit national security wiretaps without prior judicial approval would not open the door to "sweeping electronic surveillance . . . as a general law enforcement technique." He explicitly disavowed "a broad definition of national security that could cover many or most criminal investigations."

A more realistic appraisal is that the FBI and the Department of Justice were expanding the national security rubric (lately to include surveillance of domestic groups, such as the Panthers, which the previous administration refused authorization to tap) and in addition were loath to bring under the court-order procedure any of the kinds of wiretaps or eavesdrops in which they engaged before the act was passed. The only change had been that narcotics and gambling surveillances, which were probably conducted unlawfully before 1968 even under a national security standard, were now brought to a judge for a court order.

The real point is that to get a warrant you need probable cause to believe you can acquire information about a specific crime that has been committed. Probably, one former Justice Department official speculated, "they are not asking for warrants in national security cases because they are not seeking factual information on a crime and therefore they couldn't comply with the statute."

On June 19, 1972, a unanimous Supreme Court rejected the government's domestic national security exception to the Fourth Amendment. At least in certain cases, said the court, "prior judicial approval is required for . . . domestic security surveillance." The case leaves many troubling questions unanswered, but the answer it does give clearly rejects the legal theory six administrations have relied on to conduct warrantless electronic surveillance.

The 1970 wiretap report, like Sherlock Holmes' hound, is also interesting for what it does *not* show. Although the act requires a report whenever an application for surveillance is denied, the report shows no denials whatever.

Other interesting facts emerge from the year-end report of experience under the act:

1. The breakdown between wiretaps and bugs gives some clue to the FBI's methods in the past. Only three of the 180 surveillances were bugs, and five were combination bugs and taps. The other 172 were wiretaps alone. Only one of the bug installations resulted in arrests, and that was a follow-up to a surveillance order issued in 1969.

2. The average cost for 1970 was $12,106 per surveillance, which compares, for example, with the New Jersey state attorney general's average cost of a little over $2,000 per wiretap (on a total of eighty-two taps). It cost the federal government, for example, over $84,000 to tap an apartment telephone in California for 20 days and overhear 18 people engage in 266 conversations (of which 34 are listed as "incriminating," although there were no arrests). Or, to take the most successful case listed, it cost the Bureau $146,300 to listen for eighteen days in September and October, 1970, to a residence telephone in California. Forty-six persons were then arrested and twenty-one convicted, on narcotics charges.

3. Wiretaps are, of course, "general searches" in that they are totally indiscriminate and pick up innocuous private conversations of innocent people along with incriminating conversations of law violators. It was nothing less than remarkable, therefore, to read of Attorney General Mitchell's recent statement to a national meeting of police officials that "more than two out of every three messages intercepted by Federal investigators [under the 1968 act's wiretapping provisions] were incriminating . . ." The law requires prosecutors to report the number of "incriminating communications intercepted," and an analysis of the 1970 statistics shows how he got his figures.

The statistics show, for example, a tap kept for thirteen days in the latter part of 1970 on a "business-residence" in Michigan where "gambling" was suspected. Eight persons are said to have been overheard engaging in 3,655 conversations. Of these, 3,525 are listed as "incriminating intercepts." Yet under "number of persons arrested," the report lists "none." Another tap, also in Michigan, overheard only one person (is that possible?) engaged in 1,350 conversations, of which 1,300 were "incriminating." Again no arrests.

In fact, the statistical tables show an extraordinary number of gambling taps, each with a phenomenal number of "incriminating intercepts" (presumably calls placing bets or giving information) and a minuscle number of arrests in these cases. Such reports are not limited to gambling cases, or even to wiretaps. Consider, for example, the eighteen-day bug in a Michigan apartment where "extortionate credit transactions" were suspected. Twenty-two people were heard, forty-four conversations are reported to have been intercepted and twenty-four of these are listed as "incriminating." No arrests.

Indeed, the ratio of success is so phenomenal that it raises some questions about the integrity of the FBI's reporting. In only 6 of the 180 surveillances installed in 1970 were no incriminating conversations overheard. With a society as paraoid as ours on the subject of wiretapping, and with an organized crime network allegedly so sophisticated that it can outsmart ordinary crime-detection techniques, is it within the realm of possibility that so many people are talking freely about their criminal activity into the telephone or on "bugged" premises?

II: Paranoia, Confusion and Ambivalence

Hundreds of thousands of Americans—perhaps millions—are convinced that the FBI is listening in on them personally. True, there is more such surveillance going on than Hoover admitted—but not that much. Yet no matter that there are too few agents, that it takes too many to install and monitor a tap or bug, that the FBI has too many other things to do (most unrelated to electronic surveillance) or that it ,as much as any other organization in the country, is aware of the inefficiencies of tapping and bugging. Nothing can dissuade a man who wants to believe that the FBI Director personally has on a set of earphones and is monitoring his every call.

The public paranoia is not exclusively—and probably not primarily—the public's fault. When Burnett Britton, who served with the internal security section of the FBI's San Francisco office for ten years, was asked why the Bureau, with its public relations consciousness, did not do something to dispel the impression, he replied: "It's very nice to know that the people you're chasing are afraid to use telephones. In fact that's one reason why in chasing the Communist Party we didn't have to use many taps. They were scared to use telephones!"

In addition to the FBI's own reasons for promoting the notion that Big Brother may be watching you (undoubtedly offset now by the public relations reasons for denying it), a number of other variables add to and account for public confusion and misinformation.

Part of it has to do with the inherent nature of the activity—secret surveillance in an open society. Superimposed is the FBI's own cloak of secrecy and its unique freedom from the normal controls exercised over government agencies. Even the Director's boss, the Attorney General, has been, until relatively recent years, ignorant of the particulars of the FBI's electronic surveillance practices and content to permit the Bureau to conduct is own operations under the general guidelines so long as it didn't get him into any trouble. And this hands-off attitude from the nation's chief legal officers was surely encouraged, in part, by the extraordinary circumstance that the Director, with the exception of a brief three-year period under the Kennedys, had direct access to the White House and was able, more or less when the spirit moved him, to bypass the chain of command.

The FBI's independence kept not only the various Attorneys General ignorant; it obscured the facts for line government lawyers who might have flushed the issue earlier. This was because of the FBI's organizational determination not to reveal the identity of its informants, a policy which found expression in the reports and memoranda seen and used within the Justice Department. Language such as "NKT-1, a usually reliable informant, says John Smith will be arriving in New York at 10 P.M. at La Guardia airport on American Airline flight 303" might mean that Smith's travel plans had been overheard on a tapped conversation. But it did not occur to Justice Department attorneys (many of whom are young lawyers who leave after a few years on the job), until the matter became the subject of a minor scandal, that NKT-1 could as easily be an electronic informant as a live one.

One U.S. attorney recalls a meeting with an FBI agent and an assistant U.S. attorney. The assistant was pushing the agent to get more information than his report revealed, but the agent didn't have any more information. The assistant said, "But if your informant was close enough to hear what was being said, surely he can give us a description of these men?" In exasperation, the agent blurted, "The informant is blind." Retrospectively, the U.S. attorney said, "I caught it—but my assistant didn't know what the hell he was talking about."

An additional source of continuing confusion is the distinction between tapping, which is interception of a telephone conversation through a direct link-up to a telephone line, and bugging, which is microphone surveillance of a room. That distinction is critical in evaluating the legal and policy justifications for FBI practices for a number of reasons: First, under the constitutional theory which was the law of the land between 1928 and 1967, a telephone tap could almost never be unconstitutional, while microphone surveillances, which often required a "trespass" on private premises, might well be violations of the Fourth Amendment. Second, until 1968 there was no federal legislation specifically prohibiting bugging, but Section 605 of the Communications Act made interception and divulgence of telephone coversations criminal acts. Third, the FBI publicly announced that it sought the Attorney General's authorization for each and every tap it installed. But departmental procedures—until Nicholas deB. Katzenbach became Attorney General—did not involve either authorizing or notifying the Attorney General on the installation of bugs on a bug-by-bug basis.

Part of the misunderstanding today is undoubtedly a cultural lag from the days when federal law differed from state law and tapping law differed from bugging law. At one point, wiretap evidence, barred in federal courts, could be used in the courts of twenty-nine states, with the Supreme Court ruling that the Federal Communications Act made it inadmissible only in federal courts. And evidence obtained in violation of the Fourth Amendment—where a microphone was installed by trespass—could still be used in a state court.

To complicate matters further, electronic surveillance has been a principal tool of the FBI's war against those who would conduct espionage and sabotage against the country—a tool which the FBI has been encouraged to use by Franklin Delano Roosevelt and all his successors to date. It has seemed unpatriotic to question its use for national security purposes; so, again, electronic surveillance has been insulated from effective scrutiny.

In addition to all this, the public itself has been ambivalent—shocked when a congressman like Hale Boggs charges that his phone has been tapped, titillated when treated to thousands of pages of illegally overheard organized-crime telephone conversations. Such ambivalence on the part of the public and officeholders has marked the history of FBI use of electronic surveillance.

This public ambivalence has been reflected in the attitude of its representatives. Francis Biddle, in his memoir *In Brief Authority*, relates the following characteristic story of a President's responses to the discovery that the FBI was engaged in dubious electronic surveillance:

> . . . the Judiciary Committee met to hear objections from a few opposing witnesses connected with the Citizens Committee for Barry Bridges, who testified that they had watched FBI agents through binoculars from a neighboring building tap Bridges' telephone wire in New York City. There was no doubt that an FBI agent had applied the tap. Suddenly realizing that he was being watched, he made such a hasty exit that he left a letterhead identifying him with the Bureau, which was captured by the Bridges group . . . When all this came out in the newspapers I could not resist suggesting to Hoover that he tell the story of the tap directly to the President. We went over to the White House together. FDR was delighted; and with one of his great grins, intent on every word, slapped Hoover on the back when he had finished. "By God, Edgar, that's the first time you've been caught with your pants down!" The two men liked and understood each other.

III: The Lessons of the Past

In many areas the FBI has commendably been ahead of the rest of the country's law-enforcement establishment in respecting the rights of American citizens. The now much-criticized *Miranda* decision, for example, requires local officials to give the same warnings to arrested suspects that the FBI had been giving voluntarily for years—namely that all accused have the right to remain silent, that statements voluntarily made may be used against them and that they have a right to consult a lawyer. By and large FBI security over its files has been good, leakage has been the exception, rather than the rule. (The Bureau does, however, tend to make some files public indiscriminately, as Aryeh Neier pointed out with regard to arrest records.)

But the experience with FBI electronic surveillance over the past three decades gives little ground for confidence that discretion left to it—with or without the supervision of the Attorney General—will in the future be exercised in the interests of good government.

The problem was not necessarily a personal one with J. Edgar Hoover. If Hoover in his later years had a permissive attitude toward wiretapping and electronic surveillance, he may, on the basis of the record, be taken at his word that it was a technique he preferred not to use. In his earliest statement on the subject (in 1931) he said, "While it may not be illegal, I think it is unethical, and it is not permitted under the regulations by the Attorney General." He wrote to the *Harvard Law Review in* February, 1939, that wiretapping was an "archaic and inefficient" practice which "has proved a definite handicap or barrier in the development of ethical, scientific and sound investgative techniques." His Bebruary, 1949, letter to the *Yale Law Journal* quoted his earlier expressions "opposed to uncontrolled and unrestrained wiretapping by law enforcement officers."

But the best of intentions and the finest-sounding general instructions and guidelines are insufficient guarantees that the executive—even at the level of the Director, the Attorney General, the President—can be relied upon, operating in secret, to respect this or that individual's right to privacy when it conflicts with some immediate concern and apparent national priority. Whether these dangers are alleviated by *ex parte* court review is uncertain, but the history demonstrates that more control, or abolition of the practice altogether, is necessary.

A. 1920–40

Ambivalence and uncertainty began almost as soon as the art of electronic surveillance was born. After Hoover became Director in 1924, Attorney General Stone issued an order prohibiting wiretapping by the Bureau. That instruction was reaffirmed by Attorney General Sargent in 1928.

The Bureau of Prohibition was not subject to these restraints, and it broke a bootleg "conspiracy of amazing magnitude"—to use Chief Justice Toft's description—by extensive wiretaps in Seattle in 1927, and thereby gave rise to the *Olmstead* case. By 5-to-4 majority (over now-famous dissents by Justices

Brandeis and Holmes and less-well-known opinions by Justices Butler and former Attorney General Stone), the court ruled that evidence "secured by use of the sense of hearing and that only" was not unconstitutionally obtained because it was not a "search" or "seizure" as those terms are used in the Fourth Amendment.

In the meantime, in 1930, the Bureau of Prohibition was transferred to the Department of Justice, and Attorney General William D. Mitchell directed on January 19, 1931, that the bar on FBI wiretaps be withdrawn and the following department-wide language substituted:

> No tapping of wires should be permitted to any agent of the Department without the personal direction of the Chief of the Bureau involved, after consultation with the Assistant Attorney General in charge of the case.

Bills to prohibit wiretaps were introduced in the Seventy-first and Seventy-second Congresses, and hearings were held at which Attorney General Mitchell and Prohibition Director Woodcock testified. The Attorney General maintained that he had issued instructions permitting the installation of a wiretap only on "the personal direction of the Chief of the Bureau involved, after consultation with the Assistant Attorney General in charge of the case." The justification given for wiretapping by the Attorney General named Mitchell in 1931 was not much different from what his namesake said later.

The flurry of congressional debate finally culminated in a rider to the 1933 Department of Justice Appropriation Act which forbade "wiretapping to procure evidence of violations of the National Prohibition Act . . ." And with the demise of Prohibition, interest in specific legislative restraint on wiretapping waned.

But in 1934 Congress enacted the Federal Communications Act, and Section 605 of that principally regulatory law forbade the interception and disclosure of interstate telephone messages. In 1937, in *Nardone v. United States*, a prosecution for conspiracy to smuggle into the United States almost 10,000 gallons of alcohol, it developed at trial that federal agents had tapped the conspirators' phones and overheard approximately five hundred calls. Of these, seventy-two were incriminatory enough to be used directly as evidence at trial. Nine years after *Olmstead*, seven members of the Supreme Court held that the "plain words" of Section 605 forbade testimony in federal court which would divulge an intercepted telephone message. The majority opinion was written by Justice Owen Roberts.

Without explicitly overruling *Olmstead*, the court majority rejected its narrow view of privacy, observing that Section 605 may have been passed by Congress for "the same considerations . . . as evoked the guaranty against practices and procedures violative of privacy, embodied in the Fourth and Fifth Amendments of the Constitution." That rejection was confirmed two years later by the Court's second *Nardone* decision. It held that Section 605 prohibited not merely divulgence of "the exact words heard through forbidden interceptions" but also "derivative use" of such proscribed evidence. The court's understanding of *Nardone I* was that it was "not the product of a merely meticulous reading of technical language," but "the translation into practicality of broad considerations of morality and public well-being."

Arthur Krock reported in the New York *Times* (April 4, 1940) that Mr. Hoover had, after the Supreme Court decision, "asked his superiors for a ruling and was informed that wiretapping to obtain leads on criminality was not banned by the decision." This was consistent with Hoover's own statement —made after embarrassing tapping disclosures and congressional concern the following year—on FBI policy:

> The Federal Bureau of Investigation has utilized wiretapping as a method of securing information of *investigative value only* in extraordinary situations and *in an entirely legal manner*, where either a human life was st stake or where the activities of persons under investigation were of such an aggravated criminal nature as to justify the use of extraordinary means to detect their activities and cause their apprehension. [Emphasis added.]

Whatever Mr. Hoover's personal views may have been (and various statements showed him still cautious about electronic surveillance) the practice authorized by the Justice Department in the late 1930s raises serious legal and constitutional questions. Formal and informal statements and reports of the

FBI's practices and Mr. Hoover's standards in the late 1930s tend to show that the lines on what kinds of cases warranted tapping were flabby and indistinct. Combating highly organized crime syndicates was mentioned, as were kidnapping, extortion, and "*flagrant white slavery.*" (One is tempted to wonder why any "flagrant" violations require secret electronic surveillance.)

Obviously, then, the Justice Department's and FBI's view of what warranted tapping went beyond cases where "human life was at stake." How broadly Mr. Hoover exercised the discretion given him by the 1931 wiretap order has never been—and probably never will be—fully or even substantially known. Nor do we know how many individuals were sent off to jail in that period on evidence which was the fruit of wiretaps.

There was similar lack of public scrutiny of the use of bugs. The record in the *Goldman* case, which the Supreme Court decided in 1942, shows that in 1937—in an ordinary bankruptcy fraud investigation—Bureau agents were planting microphones in private rooms and listening to conversations without the agreement of any of the parties or the occupant of the premises. Apparently the limitations on wiretaps (under Section 605) to certain kinds of cases did not apply to microphone surveillances (controlled by the Fourth Amendment). Nor, indeed, was there even a requirement that a microphone surveillance be approved by the Director—possibly leaving the final decision on its installation to a SAC. Apparently, the only restriction was on disclosure, although the Fourth Amendment—unlike Section 605—has no "non-divulgence". provision.

So the FBI came to the threshold of World War II with apparent authority to tap wires on the signature of the Director and similar authority to bug in the field. Both were highly dubious—the first possibly criminal (under the Federal Communications Act) and both possibly unconstitutional. It was in this context that, in September, 1939, the FBI was given supervisory authority over investigations relating to espionage, sabotage and violations of the neutrality regulations. Its electronic surveillance activities swung into their next stage.

B. 1940–47

Robert Jackson was nominated to be Attorney General on January 4, 1940. In February, 1940, the FBI admitted wiretapping in a celebrated case, and a public outcry ensued. The Director thereupon issued the public release previously quoted. Two days later, a press release was issued out of Robert Jackson's office stating that upon the "recommendation" of Hoover, the Attorney General was repealing the 1931 authorization given by Attorney General Mitchell and superseding it with the pre-1931 language which imposed an absolute ban on "unethical tactics," including wiretapping.

The new policy did not last even a hundred days. Whether President Roosevelt was personally concerned with the effect of the no-tapping rule on espionage investigations or whether a suggestion was made by Mr. Hoover or someone else is not yet known, but on May 21, 1940, Roosevelt sent Jackson a confidential memoradnum which said:

> I have agreed with the broad purpose of the Supreme Court decision relating to wiretapping in investigations. The Court is undoubtedly sound in regard to the use of evidence secured over tapped wires in the prosecution of citizens in criminal cases and is also right in its opinion that under ordinary and normal circumstances wiretapping by Government agents should not be carried on for the excellent reason that it is almost bound to lead to abuse of civil rights.
>
> However, I am convinced that the Supreme Court never intended any dictum in the particular case which it decided to apply to grave matters involving the defense of the nation.
>
> It is, of course, well known that certain other nations have been engaged in the organization of propaganda of so-called "fifth columns" in other countries and in preparation for sabotage as well as actual sabotage.
>
> It is too late to do anything about it after sabotage, assassination and "fifth column" activities are completed.
>
> You are, therefore, authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigating agents that they are at liberty to secure information by listening devices directed to the conversation or other communications

> of persons suspected of subversive activities against the Government of the United Staes, including suspected spies. You are requested furthermore to limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens.

This document and its results tell much about the perils of delegating unwarranted electronic surveillance authority to the Director-Attorney General-President axis on national security grounds—just about the most important problem today in the area of electronic surveillance.

First and most important, the authorizing paragraph of the memorandum is rife with ambiguous and troublesome terms and phrases. Some of those which, with hindsight, appear most flagrant are:

1. "in such cases as you may approve"—Was the President intending to permit the Attorney General to define classes of cases other than the "sabotage, assassination and 'fifth column' activities" which were described in the preceding paragraph?

2. "after investigation of the need in each case"—Does this require Attorney General approval of each installation of a tap or bug or does it permit blanket surveillance authority to cover an entire investigation?

3. "to secure information"—Was this intended to limit the authority to "intelligence" activities as contrasted with investigation for prosecution?

4. "listening devices"—Were bugs, as well as taps, to be covered?

5. "directed to the conversation or other communications"—Was this intended to limit the wiretap authority to particular conversations rather than to authorize a continuing tap (particularly in light of the exhortation that it be kept "to a minimum")?

6. "persons suspected of subversive activities against . . . the United States"—Was this group to include the kind of "domestic security" cases in which the present Administration is bugging and tapping without a warrant?

Second, the difficulties growing out of its ambiguous language are compounded by the history of the memorandum. As Francis Biddle noted some years later. "The memorandum was evidently prepared in a hurry by the President personally, without consultation, probably after he had talked to Bob [Jackson]. It opened the door pretty wide to wiretapping of *anyone suspected of subversive activities.* Bob didn't like it, and not liking it, turned it over to Edgar Hoover without himself passing on each case . . ." [emphasis added].

Third, the memorandum appears singularly unconcerned with legal and constitutional problems, and treats the firm holding in the *Nardone* cases as simply "dictum."

Fourth, Jackson, being a skilled enough lawyer to know that the memorandum rested on no acceptable legal rationale, worked out a justification for the departmental practice. In March, 1941, he announced that the "only offense under [Section 605 of the Communications Act] is to intercept any communication and divulge or publish . . . Any person, with no risk of penalty, may tap telephone wires . . . and act upon what he hears or make any use of it that does not involve divulging or publication." This reasoning was very thin. It appeared to conflict with the decision in the second *Nardone* case (where evidence obtained through intragovernmental disclosure of wiretap leads was barred). And it was ultimately condemned by the organized bar.

Fifth, again seeking to shore up the legal authority for what the President had done, the Administration supported wiretap authority legislation—which it had not two years earlier. In his 1940 Attorney General's Report, Jackson urged the enactment of such a law to avoid abuse of wiretapping powers. He sent Alexander Holtzoff, as his representative, to testify in support of legislation with safeguards, although the specific bill which was first introduced by Congressman Hobbs (H.R. 2266) was thought too broad.

Sixth, in response to a request to comment on the Hobbs proposal, the President wrote Congressman Tom Eliot a letter which appeared to extend the authority of his May, 1940, memorandum to the kinds of cases which Mr. Hoover had cited in the 1930s—kidnapping and extortion.

Interestingly enough, the copy of the Eliot letter shows signs of last-minute alterations to include extortion along with kidnapping. One can fairly assume that this was done to prevent the added authority from being virtually useless. For while "extortion" may be a term that could include much of "racketeering" activity, "kidnapping" had a very definite and limited meaning. Congressman Hobbs subsequently introduced an Administration-approved measure per-

mitting the FBI to tap phones when specially authorized by the Attorney General, and making the taps admissible in evidence. The bill was reported out of the House committee, but was defeated on the floor.

A final point about the FDR memorandum to Jackson is perhaps crucial. What authority did the President have to "direct and authorize" conduct which might be a criminal act under a federal statute or—in the case of a trespassory "listening device"—might violate the Constitution? Whatever fine legal distinction the Department of Justice's lawyers were relying upon to separate impermissible divulgence from permitted tapping and bugging apparently did not enter into FDR's reckoning. Nothing in his memorandum to Jackson relates to whether the overheard conversations are or are not disclosed. Nor does it appear in the letter to Congressman Eliot.

The Roosevelt memorandum has been relied upon to this day in national security wiretaps. But no adequate answer has been given to Judge Sylvester Ryan's subsequent dismissal of the "authorization" claim in the Coplon case: "It is stated that these taps were installed 'pursuant to written authorization in each instance received from the Attorney General of the United States.' Such authorization did not clothe with legality the unlawful activities of the wiretappers nor detract at all from the interdiction of the Supreme Court on evidence secured by this type of investigation."

The FDR memorandum—with all its holes gaping—nevertheless became the authority for wartime electronic surveillance. The uncertainty about the meaning of "listening devices" was apparently resolved within the Justice Department to include only wiretaps. This meant that no Attorney General approval was required to install a bug—even when done after "trespass." So until 1965, when the whole issue got into the newspapers, whenever Hoover wanted to install a wiretap he filed an application with and secured the authorization of the Attorney General. But when he wanted to install a bug, he did so without checking with anybody. That was true even though the Supreme Court had said in the *Goldman* case that the installation by federal officers of a listening apparatus *by trespass or unlawful entry* would violate the Fourth Amendment.

C. 1947–54

A new phase began with the end of World War II and the Attorney Generalship of Tom C. Clark, President Truman's appointee. Clark, like Jackson and Biddle before him, tried to get legislative authorization for wiretaps. Before doing so, however, he sought support from Truman in a confidential memorandum in which he quoted part of one paragraph from FDR's 1940 memorandum to Robert Jackson, and added:

> It seems to me that in the present troubled period in international affairs, accompanied as it is by an increase in subversive activity here at home, it is as necessary as it was in 1940 to take the investigative measures referred to in President Roosevelt's memorandum. At the same time, the country is threatened by a very substantial increase in crime. While I am reluctant to suggest any use whatever of these special investigative measures in domestic cases, it seems to me imperative to use them in cases vitally affecting the domestic security, or where human life is in jeopardy.
>
> As so modified, I believe the outstanding directive should be continued in force. If you concur in this policy, I should appreciate it if you would so indicate at the foot of this letter.

President Truman marked "I concur" on the memorandum on July 17, 1947, and returned it to Clark. Thus the FDR memorandum was extended well beyond its intended scope. Professor Athan Theoharis of Marquette University has pointed out how this was accomplished:

> While implying that this new directive would be a simple extension of Roosevelt's policy, and thereby reducing any suspicions that Truman might have held about wiretapping and the relationship of this policy to that of his predecessor, Clark had significantly distorted the Roosevelt directive. In his quote from the operative paragraph of Roosevelt's directive, Clark had deleted its last qualifying sentence—"You are requested furthermore to limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens." Moreover, Clark's letter did not convey the essence of the Roosevelt memorandum, whether Roosevelt's concern about

> the abuse of this authority or his restriction of wiretapping to foreign activities involving sabotage. In addition, Clark's intent went significantly beyond Roosevelt's, in that he proposed that wiretapping be used to investigate domestic crime or "subversive" activities. In the absence of good staff work that would have appraised him of the specific nature of Roosevelts policy, and accepting t he assurances of his Attorney General, Truman signed the letter. By so doing, he provided the basis for a significant change in executive wiretapping policy.

Soon thereafter came the Judith Coplon case with its large bag of disclosures on FBI wiretapping. During her first trial, her attorneys demanded that full texts of FBI reports she was charged with stealing be introduced, and they showed that in fifteen of the twenty-eight, wiretap information was included. A demand that FBI agents be questioned whether Miss Coplon's phone was tapped was denied.

But in her second trail, such questioning was allowed. It revealed that forty FBI agents had tapped telephones in her Washington apartment, her office and her family's home in Brooklyn. The tapping occurred for some time before and for two months after her arrest.

The Coplon case and the public furor over it persuaded Attorney General Clark to withdraw the request for legislation authorizing wiretapping—after the Americans for Democratic Action demanded an investigation of the Justice Department's tapping practices. And at the same time—without disclosing the 1947 memorandum to Truman and the President's concurrence—Mr. Clark announced publicly: "There has been no new policy or procedure since the initial policy was stated by President Roosevelt, and this has continued to be the department's policy whenever the security of the nation is involved."

J. Howard McGrath, who followed Clark as Attorney General (serving from 1949 to 1952), announced in 1950 there would be no change in the FBI's wiretapping policy and that standards for "limited" use of wiretapping had been fixed by President Roosevelt and former Attorneys General. He also resolved bugging problems by advising the FBI in a 1952 memorandum—which has never appeared publicly—that (1) the Bureau could not install any microphones involving trespass; (2) whenever evidence in any case was referred from the Bureau to the Department where a telephone tap or microphone surveillance was used, the Bureau should inform department attorneys of that fact. But the disclosures in the Fred B. Black case, and its successors, in 1966 indicate that these instructions were simply not followed.

D. 1954–66

Attorneys General are transient but Hoover was not. So the FBI bided its time until a new Attorney General came in. Then, according to recollections of former Justice Department attorneys, immediately after the Eisenhower administration took office, the Bureau commenced negotiations with the department to erode the McGrath positions. A series of meetings took place in 1953. They apparently culminated after the Supreme Court decided the *Irvine* case, and the Bureau solicited an opinion from Attorney General Herbert Brownell to give the FBI blanket authority to install microphones by trespass.

It was this memorandum, apparently, on which the Solicitor General relied twelve years later, in the *Black* case, when he told the Supreme Court:

> Under Department practice in effect for a period of years prior to 1963, and continuing into 1965, the Director of the Federal Bureau of Investigation was given authority to approve the installation of devices such as that in question for intelligence (and not evidentiary) purposes when required in the interest of internal security or national safety, including organized crime, kidnappings, and matters wherein human life might be at stake.

The "authority" referred to so definitively has yet to be specifically identified by the Justice Department. Yet it was the basis of every FBI eavesdrop from 1954 until bugging was legalized under the Omnibus Crime Control Act of 1968. No document other than the Brownell memorandum of May 20, 1954, has surfaced. The full text of the memorandum, reprinted from *Kennedy Justice*, by Victor S. Navasky, follows:

May 20, 1954 "CONFIDENTIAL"
To: Director.
From: The Attorney General.
Subject: Microphone Surveillance.

The recent decision of the Supreme Court entitled *Irvine* v. *Calif.* 347 US 128, denouncing the use of microphone surveillances by city police in a gambling case makes appropriate a reappraisal of the use which may be made in the future by the Federal Bureau of Investigation of microphone surveillance in connection with matters relating to the internal security of the country.

It is clear that in some instances the use of microphone surveillance is the only possible way of uncovering the activities of espionage agents, possible saboteurs, and subversive persons. In such instances I am of the opinion that the national interest requires [that] microphone surveillance be utilized by the Federal Bureau of Investigation. This use need not be limited to the development of evidence for prosecution. The FBI has an intelligence function in connection with internal security matters equally as important as the duty of developing evidence for presentation to the courts and the national security requires that the FBI be able to use microphone surveillance for the proper discharge of both of such functions. The Department of Justice approves the use of microphone surveillance by the FBI under these circumstances and for these purposes. I do not consider that the decision of the Supreme Court in *Irvine* v. *California* requires a different course. That case is really distinguishable on its facts. The language of the Court, however, indicates certain uses of microphones which it would be well to avoid, if possible, even in internal security investigations. It is quite clear that in the Irvine case the Justices of the Supreme Court were outraged by what they regarded as the indecency of installing a microphone in a bedroom. They denounced the utilization of such methods of investigation in a gambling case as shocking. The Court's action is a clear indication of the need for discretion and intelligent restraint in the use of microphones by the FBI in all cases, including internal security matters. Obviously, the installation of a microphone in a bedroom or in some comparably intimate location should be avoided wherever possible. It may appear, however, that if important intelligence or evidence relating to matters connected with the national security can only be obtained by the installation of [a microphone in such a location and under such] circumstances the installation is proper and is not prohibited by the Supreme Court's decision in the Irvine case.

Previous interpretations which have been furnished to you as to what may constitute a trespass in the installation of microphones, suggest that the views expressed have been tentative in nature and have attempted to predict the course which courts would follow rather than reflect the present state of the law. It is realized that not infrequently the question of trespass arises in connection with the installation of a microphone. The question of whether a trespass is actually involved and the second question of the effect of such a trespass upon the admissibility in Court of the evidence thus obtained, must necessarily be resolved according to the circumstances of each case. The Department in resolving the problems which may arise in connection with the use of microphone surveillance will review the circumstances of each case in the light of the practical necessities of investigation and of the national interest which must be protected. It is my opinion that the Department should adopt that interpretation which will permit microphone coverage by the FBI in a manner most conducive to our national interest. I recognize that for the FBI to fulfill its important intelligence function, considerations of internal security and the national safety are paramount, and therefore, may compel the unrestricted use of the technique in the national interest.

The major references in the Brownell memorandum which might remotely be interpreted as going beyond national security are its concluding two sentences. But they are qualified by all the preceding language. And while the earlier reference to "internal security matters" is preceded by the word "including," the context of that reference indicates that it *restricts* the Bureau's use of microphones rather than expands it. By noting that the *Irvine* decision shows the need for discretion and restraint in all "use of microphones by the FBI"—"including internal security matters"—the Attorney General could hardly have been authorizing microphone installations in *other* situations.

It would, of course, be inconceivable for any closely watched organization—continually exposed to public scrutiny (as the FBI is not)—to leap on phrases like "national interest" or "national safety" in a secret document, wrench them out of context and then use them as an excuse to eavesdrop on a bookie joint in Miami. And it is difficult to accept the FBI's reliance on a memorandum that explicitly condemns the trespassory installation of a microphone in a gambler's bedroom as authority for trespassory installation of a microphone in the bedroom of a Las Vegas casino manager.

The most elementary question, however, is how the FBI could rely on a memorandum stating that the department would "review the circumstances of each case in the light of the practical necessities of the investigation and of the national interest" if Hoover did not submit bugs to the Attorney General for authorization on a case-by-case basis. Yet he did not.

In 1964 the scene shifted to the Congress and the courts. Congressional interest had been revived with the internal security frenzy of the 1950s, and again with the Kennedy administration's efforts to fight organized crime in the early 1960s. But no substantive congressional action resulted in either instance.

Meanwhile Attorney General Robert Kennedy (1961–64) listened to tapes of what he thought were local police bugs (permitted under local law) in Chicago and New York, and after great pressure, prodding, insistence and a sort of bureaucratic blackmail (described in *Kennedy Justice*) he authorized the tapping of Dr. Martin Luther King's telephone under the "national security" theory of the Jackson memo. After Robert Kennedy's death it was explained that it was not Dr. King who was the security risk, but alleged Communist party members in his entourage. And Dr. King was tapped "to protect him"—for in the absence of such a tap, which could prove Dr. King's innocence, the Bureau might disseminate derogatory charges against King that southern members of the United States Senate would use to undermine the strong civil rights bill of late 1963, which the Kennedys considered an imperative.

Hoover had earlier informed Kennedy of tapping procedures in the FBI, but not about bugs, and Kennedy did not ask about them. Both oversights reflect the etiquette which had developed over the years in the electronic surveillance business.

Kenndy's successor, Nicholas deB. Katzenbach, upon discovering that the FBI had indulged in bugging after trespass, had a meeting with Hoover. Hoover informed him that if the bugs were removed forthwith it would spell the end of the Justice Department's organized crime program. They compromised on a phase-out program for the bugs, and Katzenbach instituted a procedure whereby he was notified of exiting bugs on the same basis that he authorized taps.

On June 30, 1965, President Johnson issued a directive prohibiting the use of listening devices by agencies other than the Department of Justice, and authorized the latter to use such devices only where necessary to collect "intelligence affecting the national security."

E. 1966–68

Eavesdropping again came to public attention on May 24, 1966, when Solicitor General Thurgood Marshall filed a "Memorandum for the United States" in the Supreme Court in the criminal tax evasion case of Fred B. Black, an associate of Bobby Baker's. The memorandum told the court that FBI agents had bugged Black's hotel suite early in 1963, at approximately the time when the tax-evasion evidence was presented to a federal grand jury in Missouri. The Solicitor General took the position that the proof was not tainted by the overhearing, although conversations between Black and the lawyer representing him in the tax case were overheard.

On June 13 the court asked details on the kind of listening apparatus used, the authority under which it was installed (including "the person or persons who authorized its installation"), whether recordings existed and the time when government lawyers first learned of this information. The response was drafted in the Solicitor General's office with many personal consultations with Attorney General Katzenbach.

It admitted that there was "no specific statute or executive order . . . relied upon in the installation of the listening device in question." It stated that since 1940, wiretaps—"limited to matters involving national security or danger to human life"—have required "the specific authorization of the Attorney Gen-

eral in each instance." But, it said, there was no similar procedure until 1965 governing eavesdropping—notwithstanding "records of oral and written communications" which reflected concern by Attorneys General and the FBI Director that use of such devices should be severely limited. It then cited the previously quoted "departmental practice" of authorizing the Director to install such devices.

The court on November 7, 1966, vacated the conviction and ordered a new trial (385 U.S. 26). And a month later it did the same with another bugging case in which the Solicitor General had admitted that evidence at trial may have been tainted by trespassory eavesdropping. Many other such cases followed in the Supreme Court and in lower courts, and procedural issues were still being sorted out in late 1971.

Recognizing that the problem was becoming unmanageable, Acting Attorney General Ramsey Clark issued an instruction to the United States attorneys on November 3, 1966, in which he directed that no prosecution "go forward" until all illegally obtained evidence and its fruits were "purged."

And on June 16, 1967, he issued a detailed policy statement on tapping and bugging. In it, he reiterated that tapping "is prohibited by Presidential directive . . . whether or not the information which may be acquired through interception is intended to be used in any way or to be subsequently divulged outside the agency involved." While noting that nontrespassory eavesdropping had still not been held unconstitutional, Clark observed that there was "support for the view" that any eavesdropping on conversations in a private area was forbidden by the Fourth Amendment. Accordingly, he directed that no such surveillance be conducted without "advance written approval" from the Attorney General. National security investigations were mentioned separately as matters "to be taken up directly with the Attorney General."

Any remaining doubts about the vitality of *Olmstead* and the constitutionality of the non-trespassory eavesdropping approved in *Goldman* were laid to rest by *Katz* v. *United States*, 389 U.S. 347, decided in December, 1967. Both *Olmstead* and *Goldman* were squarely overruled, the court holding that the government's "activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied . . . and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment." And after *Katz* and *Berger* v. *New York*, 388 U.S. 41 (1967), which enumerated the necessary constitutional conditions for court ordered wiretapping, came Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

F. Lessons

The history of electronic surveillance, then, is a history of deception, confusion, ambivalence and after-the-fact rationalization, ranging from FDR's May, 1940, memorandum and February, 1941, letter to Jackson's 1941 strained interpretation of the words "intercept and divulge" to Tom Clark's overbroad 1947 note to Harry Truman to Hoover's failure to alert Robert Kennedy to the FBI's microphone surveillance procedures to Katzenbach's pragmatic decision on outstanding FBI bugs . . . The practice has been degrading to the President, the Attorney General, the Director, the FBI, the Justice Department, the men who have had to partake in it, the victims of it and ultimately the polity.

This is true regardless of the law-enforcement arguments in favor of wiretapping as a way of catching criminals. What it shows is that general standards, no matter how phrased, cannot restrain excesses if there is no outside agency to scrutinize what is being done. No matter how well-intentioned an Attorney General, no matter how distasteful wiretapping seemed to a younger Mr. Hoover, they found themselves drawn further into practices of dubious legality and constitutionality.

The men involved are not to be condemned personally. The system—the relationship between the Bureau and the department, the permanent Director and the transient Attorneys General—made it possible, probable, perhaps inevitable that without external (court-warranted) supervision, there would be vast abuses in the government's electronic surveillance. Whether or not a well-conceived warrant procedure can cure this problem, it is apparent that in its absence, the executive branch acting on its own has been irresponsible. The short experience of unilateral executive self-restraint under the 1968 Crime Act proves as much.

IV: Questions

In view of that failure and in hope of better control, these are questions for which Congress and the public ought to demand answers:

What is the extent of electronic surveillance carried on today? How much control do the President and the Attorney General exercise over the FBI's electronic surveillance practices? Is there more or less than before? Has the new law made a difference? What can be learned from the past? Should the Attorney General, the President and the Director of the FBI ever be trusted—without court supervision—to authorize electronic surveillance in the national security area?

How much tainted evidence finds its way into court without anyone being any the wiser—as a result of inter-agency cooperation in the exchange of information without divulging the manner in which the information was procured? What more has to be known before recommendations can be made along these lines?

The practice before the Supreme Court rejected a domestic national security exception to the Fourth Amendment is still important for what it tells us about the government's assumptions about its role and power in the area and because national security may again be used to justify warrantless surveillance. Did all "internal security" electronic surveillance requests automatically bypass the warrant procedure, or was a separate determination made on each case by the Attorney General? To what extent did the Nixon administration extend the national security or internal security umbrella to cover domestic organizations with an international dimension? By what standards did an agent decide to apply for a national security tap? Did Hoover ever turn him down and what standards did *he* use? How was it decided whether to go to court for a warrant?

Finally, are the provisions of the law requiring service of a notice upon an individual under surveillance and filing of an inventory being complied with? Is *any* weight given to the countervailing values of privacy protection in this area?

V: Conference Discussion

MR. ELLIFF: Among the Media documents is a summary of a wiretap on the Black Panther headquarters in Philadelphia. It raises some interesting questions about the merits of wiretapping for preventive intelligence purposes and I wonder if you'd comment on this. I'll describe it briefly.

Three or four pages of conversations are summarized. Much of this is extraneous to any preventive or general intelligence needs of the government. But the last conversation reads as follows:

"A called B who advised the neighborhood was saturated with pigs and was asked by B if the machinery was all set up for such things. A said the machinery was ready and that they had everything going for them."

It seems to me, though the wiretap here reported all kinds of irrelevant data, it did produce an immediate warning of a possible violent confrontation with the police. I was wondering how we weigh the value of that kind of warning, which, if properly used, could help a community relations officer defuse a situation that might be building up into a gunfight.

Balance the need for that sort of information against the clear risks required to obtain it, risks of public paranoia and of damage to principles of constitutional doctrine. How do we balance that?

MR. NAVASKY: That, you know, is the critical question. By what standards do you tap? How do you make that judgment?

When Ramsey Clark was Attorney General, he asked a young attorney in the department to take twelve random bugs—they were all in the organized crime area as it happened—and analyze them for their utility and effectiveness and whether other investigative techniques could have developed the same information.

The attorney came to the conclusion that they weren't worth it. But, then, everybody who considered the evidence reached the same conclusion they already had before looking at it. Most people who didn't believe in wiretapping concluded it wasn't useful. And those who did believe in it concluded it was.

So it's a very difficult problem. But one solution is to set standards and require law enforcers to go to an outside agency like a court and prove they meet the standards.

MR. LEWIN: All I want to add to that is that we have not in this paper, or I think generally, come to any firm conclusion that wiretapping under all circumstances and all conditions is unjustified. In fact, federal law authorizes it.

Certainly, at one extreme, one supposes that if a wiretap were installed on every telephone in the United States, and there were enough agents to listen in on every telephone, random wiretaps would turn up information that might be useful to law-enforcement authorities. But obviously that's an impermissible infringement on constitutional rights. So the only mechanism that has been devised thus far, and which we're constitutionally committed to, is examination by an impartial magistrate of the facts used to justify a tap. Our view is that even in national security cases, that is a mechanism that could and should be used.

I think anybody who's had anything to do with the search warrant system, however, in both federal and state courts, will tell you that the examination by an impartial magistrate is not always what the Supreme Court may think it to be. There are magistrates and judges who just rubber-stamp what's put before them. In fact, as we said, although the act requires that every eavesdropping warrant that's turned down be reported to the administrative office in the U.S. courts, there's not a single report of a warrant being turned down this year.

MR. MARSHALL: As I understand, you've been talking about taps and bugs that were authorized by someone, maybe wrongly authorized, but authorized by the Attorney General or the Director.

I think people have the impression that Bureau agents are sometimes forced, through the incentives and the pressures on them, to get the job done, to use these devices in ways that are not authorized even within the rules of the Bureau. For example, in cooperation with local authorities. Does your paper evaluate that aspect of it?

MR. NAVASKY: Yes, to some degree, but we found conflicting evidence. As our paper states, Bill Turner will tell you when he was an agent he installed unauthorized electronic surveillance. But other people deny that it goes on and will say it's not within the psychology of the FBI, it's not the way it's run. It's a very tightly run organization. But Bill Turner calls these unauthorized taps suicide taps and says every agent knows what a suicide tap is.

Now it seems to me that a more interesting question is how much the Bureau inspires other agencies to do things they're not supposed to do. If you look at the reports filed with the U.S. courts, there may be 180 federal wiretaps. But there are also 320 state and local wiretaps. The Bureau has access to these because they have contact with local law-enforcement agencies.

How many illegal taps does the FBI inspire? In 1965 it was revealed by a former member of Army intelligence that he had tapped Mrs. Roosevelt's hotel room during World War II. The newspaper report indicated that he did it at the invitation of the FBI. They asked: Can you help us?

But a lot of times this is not done. They don't say: Go tap someone's telephone. They say to the local police agency in Georgia, for example: can you tell us when Dr. King will be arriving in New York? And the local police agency in Georgia calls back a week later and says: Dr. King is coming to New York on the four-thirty plane from Atlanta on American Airlines. The Bureau's piece of paper will say, "T 3, a reliable informant, says Dr. King is arriving in New York on the four-thirty plane from Atlanta." Well, the Bureau may have silently inspired the local agency to listen in on Dr. King's travel plans, and yet the Bureau has done nothing illegal under the arrangement.

MR. BITTMAN: Mr. Navasky stated that one of the major problems with wiretapping and electronic eavesdropping is the fact that these have often resulted from unilateral decisions by the executive branch. There was no external auditing body governing the actions of the executive branch. In 1968, as I'm sure almost everyone in this room knows, Congress gave specific statutory authority for wiretapping and bugging. It has set up certain procedures governing this activity. You must get judicial approval. There are certain built-in safeguards.

Now, I have a few questions. Are you unalterably opposed to all bugging and wiretapping, whether done in national security cases or in organized crime cases? Do you believe the statute is unconstitutional? Do you believe that the requirement of judicial authority is nothing but a rubber stamp? And if you

do not belive there are sufficient safeguards, what additional safeguards would you suggest?

MR. NAVASKY: Number one. We distinguished in our paper between bugging and tapping before and after the 1968 act.

Now as of the 1968 act, which does provide procedures, I don't know whether the procedures for national security taps, as interpreted by the Attorney General and, presumably, the President, are going to hold up in court. The law has language which says, in effect, go to court and get warrants even in espionage, sabotage, treason and riot cases, among others. But then a second part of the law says the President can tap and bug without a warrant if national security is involved.

And so it's under the second part of the law that the Attorney General has found authority to allow Mr. Hoover to tap telephones in the so-called national security area, without going to court.

I would contend, number one, that as a matter of legislative intent that was not what was intended. This interpretation of the law should be struck down.

Number two, if there is a national security exception, that exception still cannot constitutionally apply to domestic groups, like the Panthers.

Number three, you asked if I believe in wiretapping and bugging under any circumstances. We were talking at lunch about that. I told Mr. Lewin that I used to think that the government ought to be able to listen in on hard-core international espionage matters. It ought to be able to listen in on "the enemy." The more I look into it, however, and the more I see how ingenious the executive branch is at going beyond the little words that lawyers and congressmen draft, the less confident I become that even this ought to be allowed.

MR. LEWIN: I think in answer to Bill Bittman's question, if I can supplement what Vic said, our concern is that the act has really made no substantial difference in restricting what the FBI does. It's expanded it instead. First, the act has given the Bureau a procedure under which it can lawfully wiretap and bug in gambling cases, narcotics cases and the entire range of cases that, before 1968, could not be justified at all. Second, in the so-called national security area, the Bureau and the Attorney General are still not going to court for judicial warrants, even where there is really no need for confidentiality. This is because the national security exception is broadly construed, thereby allowing them to keep many cases from judicial scrutiny.

So in answer to one of your questions, I'm in favor of meaningful judicial oversight of wiretapping and electronic surveillance—in other words, based on a warrant for a limited period of time. But I'm afraid that as the act is construed by the present Administration, far too many cases are excluded from its reach by the national security exception.

SUPREME COURT OF THE UNITED STATES

[Syllabus]

UNITED STATES *v.* UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF MICHIGAN ET AL.

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

No. 70–153. Argued February 24, 1972—Decided June 19, 1972

The United States charged three defendants with conspiring to destroy, and one of them with destroying, Government property. In response to the defendants' pretrial motion for disclosure of electronic surveillance information, the Government filed an affidavit of the Attorney General stating that he had approved the wiretaps for the purpose of "gather[ing] intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government." On the basis of the affidavit and surveillance logs (filed in a sealed exhibit), the Government claimed that the surveillances, though warrantless, were lawful as a reasonable exercise of presidential power to protect the national security. The District Court, holding the surveillances violative of the Fourth Amendment, issued an order for disclosure of the overheard conversations, which the Court of Appeals upheld. Title III of the Omnibus Crime Control and Safe Streets Act,

which authorizes court-approved electronic surveillance for specified crimes, contains a provisions in 18 U.S.C. § 2511(3) that nothing in that law limits the President's constitutional power to protect against the overthrow of the Government or against "any other clear and present danger to the structure or existence of the Government." The Government relies on § 2511(3) in support of its contention that "in excepting national security surveillances from the Act's warrant requirement, Congress recognized the President's authority to conduct such surveillances without prior judicial approval." *Held:*

1. Section 2511(3) is merely a disclaimer of congressional intent to define presidential powers in matters affecting national security, and is not a grant of authority to conduct warrantless national security surveillances. Pp. 4–10.

2. The Fourth Amendment (which shields private speech from unreasonable surveillance) requires prior judicial approval for the type of domestic security surveillance involved in this case. Pp. 16–23, 25.

(a) The Government's duty to safeguard domestic security must be weighed against the potential danger that unreasonable surveillances pose to individual privacy and free expression. Pp. 16–17.

(b) The freedoms of the Fourth Amendment cannot properly be guaranteed if domestic security surveillances are conducted solely within the discretion of the executive branch without the detached judgment of a neutral magistrate. Pp. 18–20.

(c) Resort to appropriate warrant procedure would not frustrate the legitimate purposes of domestic security searches. Pp. 20–23.

444 F.2d 651, affirmed.

Powell, J., delivered the opinion of the Court, in which Douglas, Brennan, Marshall, Stewart, and Blackmun, JJ., joined. Douglas, J., filed a concurring opinion. Burger, C. J., concurred in the result. White, J., filed an opinion concurring in the judgment. Rehnquist, J., took no part in the consideration or decision of the case.

SUPREME COURT OF THE UNITED STATTS

[No. 70–153]

United States, Petitioner, *v.* United States District Court for the Eastern District of Michigan, Southern Division, et al.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

June 19, 1972.

Mr. Justice Powell delivered the opinion of the Court.

The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval. Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degress,[1] without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time. Its resolution is a matter of national concern, requiring sensitivity both to the Government's right to protect itself from unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion.

This case arises from a criminal proceeding in the United States District Court for the Eastern District of Michigan, in which the United States charged three defendants with conspiracy to destroy Government property in violation of 18 U.S.C. § 371. One of the defendants, Plamondon, was charged with the dynamite bombing of an office of the Central Intelligence Agency in Ann Arbor, Michigan.

---

[1] See n. 10, *infra.*

During pretrial proceedings, the defendants moved to compel the United Statds to disclose certain electronic surveillance information and to conduct a hearing to determine whether this information "tainted" the evidence on which the indictment was based or which the Government intended to offer at trial. In response, the Government filed an affidavit of the Attorney General, acknowledging that its agents had overheard conversations in which Plamondon had participated. The affidavit also stated that the Attorney General approved the wiretaps "to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government." [2] The affidavit, together with the logs of the surveillance, were filed in a sealed exhibit for *in camera* inspection by the District Court.

On the basis of the Attorney General's affidavit and the sealed exhibit, the Government asserted that the surveillances were lawful, though conducted without prior judicial approval, as a reasonable exercise of the President's power (exercised through the Attorney General) to protect the national security. The District Court held that the surveillance violated the Fourth Amendment, and ordered the Government to make full disclosure to Plamondon of his overheard conversations. —— F. Supp. ——.

The Government then filed in the Court of Appeals for the Sixth Circuit a petition for a writ of mandamus to set aside the District Court order, which was stayed pending final disposition of the case. After concluding that it had jurisdiction,[3] that court held that the surveillances were unlawful and that the District Court had properly required disclosure of the overheard conversations, 444 F. 2d 651 (1971). We granted certorari, 403 U.S. 930.

I

Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §§ 2510–2520, authorizes the use of electronic surveillance for classes of crimes carefully specified in 18 U.S.C § 2516. Such surveillance is subject to prior court order. Section 2518 sets forth the detailed and particularized application necessary to obtain such an order as well as carefully circumscribed conditions for its use. The Act represents a comprehensive attempt by Congress to promote more effective control of crime while protecting the privacy of individual thought and expression. Much of Title III was drawn to meet the constitutional requirements for electronic surveillance enunciated by this Court in *Berger* v. *New York*, 388 U.S. 41 (1967), and *Katz* v. *United States*, 389 U.S. 347 (1967).

---

[2] The Attorney General's affidavit reads as follows:

"JOHN N. MITCHELL being duly sworn deposes and says:

"1. I am the Attorney General of the United States.

"2. This affidavit is submitted in connection with the Government's opposition to the disclosure to the defendant Plamondon of information concerning the overhearing of his conversations which occurred during the course of electronic surveillances which the Government contends were legal.

"3. The defendant Plamondon has participated in conversations which were overheard by Government agents who were monitoring wiretaps which were being employed to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government. The records of the Department of Justice reflect the installation of these wiretaps had been expressly approved by the Attorney General.

"4. Submitted with this affidavit is a sealed exhibit containing the records of the intercepted conversations, a description of the premises that were the subjects of the surveillances, and copies of the memoranda reflecting the Attorney General's express approval of the installation of the surveillances.

"5. I certify that it would prejudice the national interest to disclose the particular facts concerning these surveillances other than to the court *in camera*. Accordingly, the sealed exhibit referred to herein is being submitted solely for the court's *in camera* inspection and a copy of the sealed exhibit is not being furnished to the defendants. I would request the court, at the conclusion of its hearing on this matter, to place the sealed exhibit in a sealed envelope and return it to the Department of Justice where it will be retained under seal so that it may be submitted to any appellate court that may review this matter."

[3] Jurisdiction was challenged before the Court of Appeals on the ground that the District Court's order was interlocutory and not appealable under 28 U.S.C. § 1291. On this issue, the Court correctly held that it did have jurisdiction, relying upon the All Writs Statute, 28 U.S.C. § 1651, and cases cited in its opinion, 444 F.2d, at 655–656. No attack was made in this Court as to the appropriateness of the writ of mandamus procedure.

Together with the elaborate surveillance requirements in Title III, there is the following proviso, 18 U.S.C. § 2511(3):

"Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1103; 47 U.S.C. § 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. *Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government.* The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial, hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power." (Emphasis supplied.)

The Government relies on § 2511(3). It argues that "in excepting national security surveillances from the Act's warrant requirement Congress recognized the President's authority to conduct such surveillances without prior judicial approval." Govt. Brief, pp. 7, 28. The section thus is viewed as a recognition or affirmance of a constitutional authority in the President to conduct warrantless domestic security surveillance such as that involved in this case.

We think the language of § 2511(3), as well as the legislative history of the statute, refutes this interpretation. The relevant language is that:

> "Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect . . ."

against the dangers specified. At most, this is an implicit recognition that the President does have certain powers in the specified areas. Few would doubt this, as the section refers—among other things—to protection "against actual or potential attack or other hostile acts of a foreign power." But so far as the use of the President's electronic surveillance power is concerned, the language is essentially neutral.

Section 2511(3) certainly confers no power, as the language is wholly inappropriate for such a purpose. It merely provides that the Act shall not be interpreted to limit or disturb such power as the President may have under the Constitution. In short, Congress simply left presidential powers where it found them. This view is reinforced by the general context of Title III. Section 2511(1) broadly prohibits the use of electronic surveillance "except as otherwise specifically provided in this chapter." Subsection (2) thereof contains four specific exceptions. In each of the specified exceptions, the statutory language is as follows:

> "IT shall not be unlawful . . . to intercept" the particular type of communication described.[4]

The language of subsection (3), here involved, is to be contrasted with the language of the exceptions set forth in the preceding subsection. Rather than stating that warrantless presidential uses of electronic surveillance "shall not be unlawful" and thus employing the standard language of exception, subsection (3) merely disclaims any intention to "limit the constitutional power of the President."

The express grant of authority to conduct surveillances is found in § 2516, which authorizes the Attorney General to make application to a federal judge when surveillance may provide evidence of certain offenses. These offenses are described with meticulous care and specificity.

Where the Act authorizes surveillance, the procedure to be followed is specified in § 2518. Subsection (1) thereof requires application to a judge of competent jurisdiction for a prior order of approval, and states in detail the infor-

[4] These exceptions relate to certain activities of communication common carriers and the Federal Communications Commission, and to specified situations where a party to the communication has consented to the interception.

mation required in such application.[5] Subsection (3) prescribes the necessary elements of probable cause which the judge must find before issuing an order authorizing an interception. Subsection (4) sets forth the required contents of such an order. Subsection (5) sets strict time limits on an order. Provision is made in subsection (7) for "an emergency situation" found to exist by the Attorney General (or by the principal prosecuting attorney of a State) "with respect to conspiratorial activities threatening the national security interest." In such a situation, emergency surveillance may be conducted "if an application for an order approving the interception is made . . . within 48 hours." If such an order is not obtained, or the application therefor is denied, the interception is deemed to be a violation of the Act.

In view of these and other interrelated provisions delineating permissible interceptions of particular criminal activity upon carefully specified conditions, it would have been incongruous for Congress to have legislated with respect to the important and complex area of national security in a single brief and nebulous paragraph. This would not comport with the sensitivity of the problem involved or with the extraordinary care Congress exercised in drafting other sections of the Act. We therefore think the conclusion inescapable that Congress only intended to make clear that the Act simply did not legislate with respect to national security surveillances.[6]

The legislative history of § 2511(3) supports this interpretation. Most relevant is the colloquy between Senators Hart, Holland, and McClellan on the Senate floor:

"Mr. Holland. . . . The section [2511(3)] from which the Senate [Hart] has read does not affirmatively give any power. . . . *We are not affirmatively conferring any power upon the President.* We are simply saying that nothing herein shall limit such power as the President has under the Constitution. . . . We certainly do not grant him a thing.

"There is nothing affirmative in this statement.

"Mr. McClellan. Mr. President, *we make it understood that we are not trying to take anything away from him.*

"Mr. Holland. The Senator is correct.

"Mr. Hart. Mr. President, there is no intention here to expand by this language a constitutional power. Clearly we could not do so.

"Mr. McClellan. Even though we intended, we could not do so.

---

[5] 18 U.S.C. § 2518, subsection (1) reads as follows:

"§ 2518. Procedure for interception of wire or oral communications.

"(1) Each application for an order authorizing or approving the interception of a wire or oral communication shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

"(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

"(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

"(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

"(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

"(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire or oral communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

"(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results."

[6] The final sentence of § 2511(3) states that the contents of an interception "by authority of the President in the exercise of the foregoing powers may be received in evidence . . . only where such interception was reasonable. . . ." This sentence seems intended to assure that when the President conducts lawful surveillance—pursuant to whatever power he may possess—the evidence is admissible.

"Mr. Hart. . . . However, we are agreed that this language should not be regarded as intending to grant any authority, including authority to put a bug on, that the President does not have now.

"In addition, Mr. President, *as I think our exchange makes clear, nothing in Section 2511(3) even attempts to define the limits of the President's national security power under present law, which I have always found extremely vague. . . . Section 2511(3) merely says that if the President has such a power, then its exercise is in no way affected by title III.* (Emphasis supplied.) [7]

One could hardly except a clearer expression of congressional neutrality. The debate above explicitly indicates that nothing in § 2511(3) was intended to *expand* or to *contract* or to *define* whatever presidential surveillance powers existed in matters affecting the national security. If we could accept the Government's characterization of § 2511(3) as a congressionally prescribed exception to the general requirement of a warrant, it would be ncessary to consider the question of whether the surveillance in this case came within the exception and, if so, whether the statutory exception was itself constitutionally valid. But viewing § 2511(3) as a congressional disclaimer and expression of neutrality, we hold that the statute is not the measure of the executive authority asserted in this case. Rather, we must look to the constitutional powers of the President.

II

It is important at the outset to emphasize the limited nature of the question before the Court. This case raises no constitutional challenge to electronic surveillance as specifically authorized by Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Nor is there any question or doubt as to the necessity of obtaining a warrant in the surveillance of crimes unrelated to the national security interest. *Katz* v. *United States*, 389 U.S. 347 (1967); *Berger* v. *New York*, 388 U.S. 41 (1967). Further, the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country. The Attorney General's affidavit in this case states that the surveillances were "deemed necessary to protect the nation from attempts of *domestic organizations* to attack and subvert the existing structure of Government" (emphasis supplied). There is no evidence of any involvement, directly or indirectly, of a foreign power.[8]

Our present inquiry, though important, is therefore a narrow one. It addresses a question left open by *Katz*, *supra*, *p.* 358, n. 23:

"Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security. . . ."

The determination of this question requires the essential Fourth Amendment inquiry into the "reasonableness" of the search and seizure in question, and

---

[7] Cong. Rec. Vol. 114, pt. 11, p. 14751, May 23, 1968. Senator McClellan was the sponsor of the bill. The above exchange constitutes the only time that § 2511(3) was expressly debated on the Senate or House floor. The Report of the Senate Judiciary Committee is not so explicit as the exchange on the floor, but it appears to recognize that under § 2511(3) the national security power of the President—whatever it may be—is not to be deemed disturbed." S. Rep. No. 1097, 90th Cong., 2d Sess., 94 (1968). See also The "National Security Wiretap": Presidential Prerogative or Judicial Responsibility where the author concludes that in § 2511(3) "Congress took what amounted to a position of neutral noninterference on the question of the constitutionality of warrantless national security wiretaps authorized by the President." 45 S. Cal. L. Rev. —— (1972).

[8] Section 2511(3) refers to "the constitutional power of the President" in two types of situations: (i) where necessary to protect against attack, other hostile acts or intelligence activities of a "foreign power"; or (ii) where necessary to protect against the overthrow of the Government or other clear and present danger to the structure or existence of the Government. Although both of the specified situations are some times referred to as "national security" threats, the term "national security" is used only in the first sentence of § 2511(3) with respect to the activities of foreign powers. This case involves only the second sentence of § 2511(3), with the threat emanating—according to the Attorney General's affidavit—from "domestic organizations." Although we attempt no precise definition, we use the term "domestic organization" in this opinion to mean a group or organization (whether formally or informally constituted) composed of citizens of the United States and which has no significant connection with a foreign power, its agents or agencies. No doubt there are cases where it will be difficult to distinguish between "domestic" and "foreign" unlawful activities directed against the Government of the United States where there is collaboration in varying degrees between domestic groups or organizations and agents or agencies of foreign powers. But this is not such a case.

the way in which that "reasonablenss" derives content and meaning through reference to the warrant clause. *Coolidge* v. *New Hampshire*, 403 U.S. 443, 473–484 (1971).

We begin the inquiry by noting that the President of the United States has the fundamental duty, under Art. II, § 1, of the Constitution, "to preserve, protect, and defend the Constitution of the United States." Implicit in that duty is the power to protect our Government against those who would subvert or overthrow it by unlawful means. In the discharge of this duty, the President —through the Attorney General—may find it necessary to employ electronic surveillance to obtain intelligence information on the plans of those who plot unlawful acts against the Government.[9] The use of such surveillance in internal security cases has been sanctioned more or less continuously by various Presidents and Attorneys General since July 1946.[10] Herbert Brownell, Attorney General under President Eisenhower, urged the use of electronic surveillance both in internal and international security matters on the grounds that those acting against the Government

> "turn to the telphone to carry on their intrigue. The success of their plans frequently rests upon piecing together shreds of information received from many sources and many nests. The participants in the conspiracy are often dispersed and stationed in various strategic positions in government and industry throughout the country." [11]

Though the Government and respondents debate their seriousness and magnitude, threats and acts of sabotage against the Government exist in sufficient number to justify investigative powers with respect to them.[12] The covertness and complexity of potential unlawful conduct against the Government and the necessary dependency of many conspirators upon the telephone make electronic surveillance an effective investigatory instrument in certain circumstances. The marked acceleration in technological developments and sophistication in their use have resulted in new techniques for the planning, commission and concealment of criminal activities. It would be contrary to the public interest for Government to deny to itself the prudent and lawful employment of those very techniques which are employed against the Government and its law abiding citizens.

It has been said that "the most basic function of any government is to provide for the security of the individual and of his property." *Miranda* v. *Arizona*, 384 U.S. 436, 539 (1966) (WHITE J., dissenting). And unless Government safeguards its own capacity to function and to preserve the security of its people, soeciety itself could become so disordered that all rights and liberties

---

[9] Enactment of Title III reflects congressional recognition of the importance of such surveillance in combatting various types of crime. Frank S. Hogan, District Attorney for New York County for over 25 years, described telephonic interception, pursuant to court order, as "the single most valuable weapon in law enforcement's fight against organized crime." Cong. Rec. Vol. 117, S. 6476, May 10, 1971. The "Crime" Commission appointed by President Johnson noted that "the great majority of law enforcement officials believe that the evidence necessary to bring criminal sanctions to bear consistently on the higher echelons of organized crime will not be obtained without the aid of electronic surveillance techniques. They maintain these techniques are indispensable to develop adequate strategic intelligence concerning organized crime, to set up specific investigations, to develop witnesses, to corroborate their testimony, and to serve as substitutes for them—each a necessary step in the evidence-gathering process in organized crime investigations and prosecutions. Report by the President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society, p. 201 (1967).

[10] In that month Attorney General Tom Clark advised President Truman of the necessity of using wiretaps "in cases vitally affecting the domestic security." In May 1940 President Roosevelt had authorized Attorney General Jackson to utilize wiretapping in matters "involving the defense of the nation," but it is questionable whether this language was meant to apply to solely domestic subversion. The nature and extent of wiretapping apparently varied under different administrations and Attorneys General, but except for the sharp curtailment under Attorney General Ramsey Clark in the latter years of the Johnson administration, electronic surveillance has been used both against organized crime and in domestic security cases at least since the 1946 memorandum from Clark to Truman. Govt. Brief, pp. 16–18; Resp. Brief, pp. 51–56: Cong. Rec. Vol. 117, S 6476–6477, May 10, 1971.

[11] Brownell, The Public Security and Wire Tapping, 39 Cornell L. Q. 195, 202(1954). See also Rogers, The Case For Wire Tapping, 63 Yale L. J. 792 (1954).

[12] The Government asserts that there were 1,562 bombing incidents in the United States from January 1, 1971, to July 1, 1971, most of which involved Government related facilities. Respondents dispute these statistics as incorporating many frivolous incidents as well as bombings against nongovernmental facilities. The precise level of this activity, however, is not relevant to the disposition of this case. Govt. Brief, p. 18; Resp. Brief, p. 26–29; Govt. Reply Brief, p. 13.

would be endangered. As Chief Justice Hughes reminded us in *Cox* v. *New Hampshire*, 312 U.S. 569, 574 (1940):

"Civil liberties, as guaranteed by the Constitution, imply the existence of an organized society maintaining public order without which liberty itself would be lost in the excesses of unrestrained abuses."

But a recognition of these elementary truths does not make the employment by Government of electronic surveillance a welcome development—even when employed with restraint and under judicial supervision. There is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens.[13] We look to the Bill of Rights to safeguard this privacy. Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance. *Katz* v. *United States*, *supra*; *Berger* v. *New York*, *supra*; *Silverman* v. *United States*, 365 U.S. 505 (1961). Our decision in *Katz* refused to lock the Fourth Amendment into instances of actual physical trespass. Rather, the Amendment governs "not only the seizure of tangible items, but extends as well to the recording of oral statements 'without any technical trespass under . . . local property law.' " *Katz*, *supra*, at 353. That decision implicitly recognized that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails[14] necessitate the application of Fourth Amendment safeguards.

National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. "Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power," *Marcus* v. *Search Warrant*, 367 U.S. 717, 724 (1961). History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent. Senator Hart addressed this dilemma in the floor debate on § 2511(3):

> "As I read it—and this is my fear—we are saying that the President, on his motion, could declare—name your favorite poison—draft dodgers, Black Muslims, the Ku Klux Klan, or civil rights activists to be a clear and present danger to the structure or existence of the Government." [15]

The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.

III

As the Fourth Amendment is not absolute in its terms, our task is to examine and balance the basic values at stake in this case: the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression. If the legitimate

---

[13] Professor Alan Westin has written on the likely course of future conflict between the value of privacy and the "new technology" of law enforcement. Much of the book details techniques of physical and electronic surveillance and such possible threats to personal privacy as psychological and personality testing and electronic information storage and retrieval. Not all of the contemporary threats to privacy emanate directly from the pressures of crime control. A. Westin, Privacy and Freedom (1967).

[14] Though the total number of intercepts authorized by state and federal judges pursuant to Tit. III of the 1968 Omnibus Crime Control and Safe Streets Act was 597 in 1970, each surveillance may involve interception of hundreds of different conversations. The average intercept in 1970 involved 44 people and 655 conversations, of which 295 or 45% were incriminating. Cong. Rec. Vol. 117, S 6477, May 10, 1971.

[15] Cong. Rec. Pol. 114, pt. 11, p. 14750, May 23, 1968. The subsequent assurances, quoted in part I of the opinion, that § 2511(3) implied no statutory grant, contraction, or definition of presidential power eased the Senator's misgivings.

need of Government to safeguard domestic security requires the use of electronic surveillance, the question is whether the needs of citizens for privacy and free expression may not be better protected by requiring a warrant before such surveillance is undertaken. We must also ask whether a warrant requirement would unduly frustrate the efforts of Government to protect itself from acts of subversion and overthrow directed against it.

Though the Fourth Amendment speaks broadly of "unreasonable searches and seizures," the definition of "reasonableness" turns, at least in part, on the more specific commands of the warrant clause. Some have argued that "the relevant test is not whether it was reasonable to procure a search warrant, but whether the search was reasonable," *United States* v. *Rabinowitz*, 339 U.S. 56, 66 (1950).[16] This view, however, overlooks the second clause of the Amendment. The warrant clause of the Fourth Amendment is not dead language. Rather it has been

> "a valued part of our constitutional law for decades, and it has determined the result in scores and scores of cases in the courts all over this country. It is not an inconvenience to be somehow 'weighed' against the claims of police efficiency. It is, or should be, an important working part of our machinery of government, operating as a matter of course to check the 'well-intentioned but mistakenly overzealous executive officers' who are a part of any system of law enforcement." *Coolidge* v. *New Hampshire*, *supra*, at 491.

See also *United States* v. *Rabinowitz*, 339 U.S. 57, 68 (1950) (Frankfurter, J. dissenting); *Davis* v. *United States*, 328 U.S. 582, 604 (Frankfurter, J., dissenting).

Over two centuries ago, Lord Mansfield held that common law principles prohibited warrants that ordered the arrest of unnamed individuals whom the *officer* might conclude were guilty of seditious libel. "It is not fit," said Mansfield, "that the receiving or judging of the information ought to be left to the discretion of the officer. The magistrate ought to judge; and should give certain directions to the officer." *Leach* v. *Three of the King's Messengers*, How. St. Tr. 1001, 1027 (1765).

Lord Mansfield's formulation touches the very heart of the Fourth Amendment directive: that where practical, a governmental search and seizure should represent both the efforts of the officer to gather evidence of wrongful acts and the judgment of the magistrate that the collected evidence is sufficient to justify invasion of a citizen's private premises or conversation. Inherent in the concept of a warrant is its issuance by a "neutral and detached magistrate." *Coolidge* v. *New Hampshire*, *supra*, at 453; *Katz* v. *United States*, *supra*, at 356. The further requirement of "probable cause" instructs the magistrate that baseless searches shall not proceed.

These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the executive branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility is to enforce the laws, to investigate and to prosecute. *Katz* v. *United States*, *supra*, at 359–360 (DOUGLAS, J., concurring). But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.[17]

It may well be that, in the instant case, the Government's surveillance of Plamondon's conversations was a reasonable one which readily would have gained prior judicial approval. But this Court "has never sustained a search

---

[16] This view has not been accepted. In *Chimel* v. *California*, 395 U.S. 752 (1969), the Court considered the Government's contention that the search be judged on a general "reasonableness" standard without reference to the warrant clause. The Court concluded that argument was "founded on little more than a subjective view regarding the acceptability of certain sorts of police conduct, and not on considerations relevant to Fourth Amendment interests. Under such an unconfined analysis, Fourth Amendment protection in this area would approach the evaporation point." *Chimel*, *supra*, at 764–765.

[17] Lasson, The History and Development of the Fourth Amendment to the United States Constitution, 79–105 (1937).

upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end." *Katz*, *supra*, at 356–357. The Fourth Amendment contemplates a prior judicial judgment,[18] not the risk that executive discretion may be reasonably exercised. This judicial role accords with our basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government. John M. Harlan, Thoughts at a Dedication: Keeping the Judicial Function in Balance, 49 A.B.A.J. 943–944 (1963). The independent check upon executive discretion is not satisfied, as the Government argues, by "extremely limited" post-surveillance judicial review.[19] Indeed, post-surveillance review would never reach the surveillances which failed to result in prosecutions. Prior review by a neutral and detached magistrate is the time tested means of effectuating Fourth Amendment rights. *Beck* v. *Ohio*, 379 U.S 89, 96 (1964).

It is true that there have been some exceptions to the warrant requirement. *Chimel* v. *California*, 395 U.S. 752 (1969); *Terry* v. *Ohio*, 392 U.S. 1 (1968); U.S. 132 (1925). But those exceptions are few in number and carefully delineated. *Katz*, *supra*, at 357; in general they serve the legitimate needs of law enforcement officers to protect their own well-being and preserve evidence from destruction. Even while carving out those exceptions, the Court has reaffirmed the principle that the "police must, whenever practicable, obtain advance judicial approval of searches and seizures through the warrant procedure," *Terry* v. *Ohio*, *supra*, at 20; *Chimel* v. *California*, *supra*, at 762.

The Government argues that the special circumstances applicable to domestic security surveillances necessitate a further exception to the warrant requirement. It is urged that the requirement of prior judicial review would obstruct the President in the discharge of his constitutional duty to protect domestic security. We are told further that these surveillances are directed primarily to the collecting and maintaining of intelligence with respect to subversive forces, and are not an attempt to gather evidence for specific criminal prosecutions. It is said that this type of surveillance should not be subject to traditional warrant requirements which were established to govern investigation of criminal activity, not on-going intelligence gathering. Govt. Brief, pp. 15–16, 23–24. Govt. Reply Brief, pp. 2–3.

The Government further insists that courts "as a practical matter would have neither the knowledge nor the techniques necessary to determine whether there was probable cause to believe that surveillance was necessary to protect national security." These security problems, the Government contends, involve "a large number of complex and subtle factors" beyond the competence of courts to evaluate. Govt. Reply Brief, p. 4.

As a final reason for exemption from a warrant requirement, the Government believes that disclosure to a magistrate of all or even a significant portion of the information involved in domestic security surveillances "would create serious potential dangers to the national security and to the lives of informants and agents. . . . Secrecy is the essential ingredient in intelligence gathering; requiring prior judicial authorization would create a greater 'danger of leaks . . . , because in addition to the judge, you have the clerk, the stenographer and some other official like a law assistant or bailiff who may be apprised of the nature' of the surveillance." Govt. Brief, pp. 24–25.

These contentions in behalf of a complete exemption from the warrant requirement, when urged on behalf of the President and the national security in its domestic implications, merit the most careful consideration. We certainly do not reject them lightly, especially at a time of worldwide ferment and when civil disorders in this country are more prevalent than in the less turbulent periods of our history. There is, no doubt, pragmatic force to the Government's position.

---

[18] We use the word "judicial" to connote the traditional Fourth Amendment requirement of a neutral and detached magistrate.

[19] The Government argues that domestic security wiretaps should be upheld by courts in post surveillance review "unless it appears that the Attorney General's determination that the proposed surveillance relates to a national security matter is arbitrary and capricious, *i.e.*, that it constitutes a clear abuse of the broad discretion that the Attorney General has to obtain all information that will be helpful to the President in protecting the Government . . ." against the various unlawful acts in § 2511(3). Govt. Brief, p. 22.

But we do not think a case has been made for the requested departure from Fourth Amendment standards. The circumstances described do not justify complete exemption of domestic security surveillance from prior judicial scrutiny. Official surveillance, whether its purpose be criminal investigation or on-going intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent. We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure.

We cannot accept the Government's argument that internal security matters are too subtle and complex for judicial evaluation. Courts regularly deal with the most difficult issues of our society. There is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases. Certainly courts can recognize that domestic security surveillance involves different considerations from the surveillance of ordinary crime. If the threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance.

Nor do we believe prior judicial approval will fracture the secrecy essential to official intelligence gathering. The investigation of criminal activity has long involved imparting sensitive information to judicial officers who have respected the confidentialities involved. Judges may be counted upon to be especially conscious of security requirements in national security cases. Title III of the Omnibus Crime Control and Safe Streets Act already has imposed this responsibility on the judiciary in connection with such crimes as espionage, sabotage and treason, § 2516(1)(a)(c), each of which may involve domestic as well as foreign security threats. Moreover, a warrant application involves no public or adversary proceedings: it is an *ex parte* request before a magistrate or judge. Whatever security dangers clerical and secretarial personnel may pose can be minimized by proper administrative measures, possibly to the point of allowing the Government itself to provide the necessary clerical assistance.

Thus, we conclude that the Government's concerns do not justify departure in this case from the customary Fourth Amendment requirement of judicial approval prior to initiation of a search or surveillance. Although some added burden will be imposed upon the Attorney General, this inconvencience is justified in a free society to protect constitutional values. Nor do we think the Government's domestic surveillance powers will be impaired to any significant degree. A prior warrant establishes presumptive validity of the surveillance and will minimize the burden of justification in post-surveillance judicial review. By no means of least importance will be the reassurance of the public generally that indiscriminate wiretapping and bugging of law-abiding citizens cannot occur.

IV

We emphasize, before concluding this opinion, the scope of our decision. As stated at the outset, this case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents.[20] Nor does our decision rest on the language of § 2511(3) or any other section of Title III of the Omnibus Crime Control and Safe Streets Act of 1968. That Act does not attempt to define or delineate the powers of the President to meet domestic threats to the national security.

Moreover, we do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case. We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of

[20] See n. 8, *supra*. For the view that warrantless surveillance, though impermissible in domestic security cases, may be constitutional where foreign powers are involved, see *United States* v. *Smith*, —— F. Supp. —— (1971); and American Bar Association Criminal Justice Project, Standards Relating to Electronic Surveillance, Feb. 1971, pp. 11, 120, 121. See also *United States* v. *Clay*, 430 F.2d 165 (1970).

security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.

Given these potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citiznes. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection. As the Court said in *Camara* v. *Municiapl Court*, 387 U.S. 523, 534–535 (1967):

> "In cases in which the Fourth Amendment requires that a warrant to search be obtained, 'probable cause' is the standard by which a particular decision to search is tested against the constitutional mandate of reasonableness. . . . In determining whether a particular inspection is reasonable—and thus in determining whether there is probable cause to issue a warrant for that inspection—the need for the inspection must be weighed in terms of these reasonable goals of law enforcement."

It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of § 2518 but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court (*e.g.*, the District Court or Court of Appeals for the Disrict of Columbia); and that the time and reporting requirements need not be so strict as those in §2518.

The above paragraph does not, of course, attempt to guide the congressional judgment but rather to delineate the present scope of our own opinion. We do not attempt to detail the precise standards for domestic security warrants any more than our decision in *Katz* sought to set the refined requirements for the specified criminal surveillances which now constitute Title III. We do hold, however, that prior judicial approval is required for the type of domestic security surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.

V

As the surveillance of Plamondon's conversations was unlawful, because conducted without prior judicial approval, the courts below correctly held that *Alderman* v. *United States*, 394 U.S. 168 (1969), is controlling and that it requires disclosure to the accused of his own impermissibly intercepted conversations. As stated in *Alderman*, "the trial court can and should, where appropriate, place a defendant and his counsel under enforceable orders against unwarranted disclosure of the materials which they may be entitled to inspect." 394 U.S. 185.[21]

The judgment of the Court of Appeals is hereby

Affirmed.

THE CHIEF JUSTICE concurs in the result.

MR. JUSTICE REHNQUIST took no part in the consideration or decision of this case.

---

[21] We think it unnecessary at this time and on the facts of this case to consider the arguments advanced by the Government for a re-examination of the basis and scope of the Court's decision in *Alderman*.

SUPREME COURT OF THE UNITED STATES

[No. 70–153]

UNITED STATES, PETITIONER, *v.* UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF MICHIGAN, SOUTHERN DIVISION, ET AL.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

JUNE 19, 1972.

MR. JUSTICE WHITE, concurring in the judgment.

This case arises out of a two-count indictment charging conspiracy to injure and injury to Government property. Count I charged Robert Plamondon and two codefendants with conspiring with a fourth person to injure Government property with dynamite. Count II charged Plamondon alone with dynamiting and injuring Government property in Ann Arbor, Michigan. The defendants moved to compel the United States to disclose, among other things, any logs and records of electronic surveillance directed at them, at unindicted coconspirators, or at any premises of the defendants or coconspirators. They also moved for a hearing to determine whether any electronic surveillance disclosed had tainted the evidence on which the grand jury indictment was based and which the Government intended to use at trial. They asked for dismissal of the indictment if such taint were determined to exist. Opposing the motion, the United States submitted an affidavit of the Attorney General of the United States disclosing that "[t]he defendant Plamondon had participated in conversations which were overheard by Government agents who were monitoring wiretaps which were being employed to gather intelligence information deemed necessary to protect the Nation from attempts of domestic organizations to attack and subvert the existing structure of the Government," the wiretaps having been expressly approved by the Attorney General. The records of the intercepted conversations and copies of the memorandum reflecting the Attorney General's approval were submitted under seal and solely for the Court's *in camera* inspection.[1]

As characterized by the District Court, the position of the United States was that the electronic monitoring of Plamondon's conversations without judicial warrant was a lawful exercise of the power of the President to safeguard the national security. The District Court granted the motion of defendants, holding that the President had no constitutional power to employ electronic surveillance without warrant to gather information about domestic organizations. Absent probable cause and judicial authorization, the challenged wiretap infringed Plamondon's Fourth Amendment rights. The court ordered the Government to disclose to defendants the records of the monitored conversations and directed that a hearing be held to determine the existence of taint either in the indictment or in the evidence to be introduced at trial.

The Government's petition for mandamus to require the District Court to vacate its order was denied by the Court of Appeals. 444 F. 2d 651 (1971). That court held that the Fourth Amendment barred warrantless electronic surveillance of domestic organizations even if at the direction of the President. It agreed with the District Court that because the wiretaps involved were therefore constitutionally inform, the United States must turn over to defendants the records of overheard conversations for the purpose of determining whether the Government's evidence was tainted.

[1] The Attorney General's affidavit concluded:
"I certify that it would prejudice the national interest to disclose the particular facts concerning these surveillances other than to the court *in camera*. Accordingly, the sealed exhibit referred to herein is being submitted solely for the court's *in camera* inspection and a copy of the sealed exhibit is not being furnished to the defendants. I would request the court, at the conclusion of its hearing on this matter, to place the sealed exhibit in a sealed envelope and return it to the Department of Justice where it will be retained under seal so that it may be submitted to any appellate court that may review this matter." App. 20–21.

I would affirm the Court of Appeals but on the statutory ground urged by respondent Keith (Brief, p. 115) without reaching or intimating any views with respect to the constitutional issue decided by both the District Court and the Court of Appeals.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 212, 18 U.S.C. §§ 2510–2520, forbids under pain of criminal penalties and civil actions for damages any wiretapping or eavesdropping not undertaken in accordance with specified procedures for obtaining judicial warrants authorizing the surveillance. Section 2511(1) establishes a general prohibition against electronic eavesdropping "except as otherwise specifically provided" in the statute. Later sections provide detailed procedures for judicial authorization of official interceptions of oral comunications; when these procedures are followed the interception is not subject to the prohibitions of § 2511(1). Section 2511(2), however, specifies other situations in which the general prohibitions of § 2511(1) do not apply. In addition, § 2511(3) provides that

> "Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1103; 47 U.S.C. § 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemd to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power."

It is this subsection that lies at the heart of this case.

The interception here was without judicial warrant, it was not covered by the provisions of § 2511(2) and it is too clear for argument that it is illegal under § 2511(1) unless it is saved by § 2511(3). The majority asserts that § 2511(3) is a "disclaimer" but not an "exception." But however it is labeled, it is apparent from the face of the section and its legislative history that if this interception is one of those described in § 2511(3), it is not reached by the statutory ban on unwarranted electronic eavesdropping.[2]

The defendants in the District Court moved for the production of the logs of any electronic surveillance to which they might have been subjected. The Government responded that conversations of Plamondon had been intercepted but took the position that turnover of surveillance records was not necessary because the interception complied with the law. Clearly, for the Government to prevail it was necessary to demonstrate first that the interception involved was not subject to the statutory requirement of judicial approval for wiretapping because the surveillance was within the scope of § 2511(3); and, secondly, if the Act did not forbid the warrantless wiretap, that the surveillance was consistent with the Fourth Amendment.

---

[2] I cannot agree with the majority's analysis of the import of § 2511(3). Surely, Congress meant at least that if a court determined that in the specified circumstances the President could constitutionally intercept communications without a warrant, the general ban of § 2511(1) would not apply. But the limitation on the applicability of § 2511(1) was not open-ended; it was confined to those situations which § 2511(3) specifically described. Thus, even assuming the constitutionality of a warrantless surveillance authorized by the President to uncover private or official graft forbidden by federal statute, the interception would be illegal under § 2511(1) because it is not the type of presidential action saved by the Act by the provision of § 2511(3). As stated in the text and footnote 3, the United States does not claim that Congress is powerless to require warrants for surveillances which the President otherwise would not be barred by the Fourth Amendment from undertaking without a warrant.

The United States has made no claim in this case that the statute may not constitutionally be applied to the surveillance at issue here.[3] Nor has it denied that to comply with the Act the surveillance must either be supported by a warrant or fall within the bounds of the exceptions provided by § 2511(3). Nevertheless, as I read the opinions of the District Court and the Court of Appeals, neither court stopped to inquire whether the challenged interception was illegal under the statute but proceeded directly to the constitutional issue without adverting to the time-honored rule that courts should abjure constitutional issues except where necessary to decision of the case before them. *Ashwander* v. *Tennessee Valley Authority*, 297 U.S. 288, 346–347 (1936) (concurring opinion). Because I conclude that on the record before us the surveillance undertaken by the Government in this case was illegal under the statute itself, I find it unnecessary, and therefore improper, to consider or decide the constitutional questions which the courts below improvidently reached.

The threshold statutory question is simply put: Was the electronic surveillance undertaken by the Government in this case a measure deemed necessary by the President to implement either the first or second branch of the exception carved out by § 2511(3) to the general requirement of a warrant?

The answer, it seems to me, must turn on the affidavit of the Attorney General offered by the United States in opposition to defendants' motion to disclose surveillance records. It is apparent that there is nothing whatsoever in this affidavit suggesting that the surveillance was undertaken within the first branch of the § 2511(3) exception, that is, to protect against foreign attack, to gather foreign intelligence or to protect national security information. The sole assertion was that the monitoring at issue was employed to gather intelligence information "deemed necessary to protect the Nation from attempts of domestic organizations to attack and subvert the existing structure of the Government." App. 20.

Neither can I conclude from this characterization that the wiretap employed here fell within the exception recognized by the second sentence of § 2511(3); for it utterly fails to assume responsibility for the judgment that Congress demanded: that the surveillance was necessary to prevent overthrow by force or other unlawful means or that there was any other clear and present danger to the structure or existence of the Government. The affidavit speaks only of attempts to attack or subvert; it makes no reference to force or unlawfulness; it articulates no conclusion that the attempts involved any clear and present danger to the existence or structure of the Government.

The shortcomings of the affidavit when measured against § 2511(3) are patent. Indeed, the United States in oral argument conceded no less. The specific inquiry put to Government counsel was: "[D]o you think the affidavit, standing alone, satisfies the Safe Streets Act?" The Assistant Attorney General

---

[3] See the Transcript of Oral Argument in this Court, pp. 13–14:

"Q. . . . I take it from your answer that Congress could forbid the President from doing what you suggest he has the power to do in this case?

"Mr. Mardian [Assistant Attorney General]: That issue is not before this Court—

"Q. Well, I would—my next question will suggest that it is. Would you say, though, that Congress could forbid the President?

"Mr. Mardian: I think under the rule announced by this court in *Colony Catering* that within certain limits the Congress could severely restrict the power of the President in this area.

"Q. Well, let's assume Congress says, then, that the Attorney General, or the President may authorize the Attorney General in specific situations to carry out electronic surveillance if the Attorney General certifies that there is a clear and present danger to the security of the United States?

"Mr. Mardian: I think that Congress has already provided that, and——

"Q. Well, would you say that Congress would have the power to limit surveillances to situations where those conditions were satisfied?

"Mr. Mardian: Yes, I would—I would concur in that, Your Honor."

A colloquy appearing in the debates on the bill, appearing at Cong. Rec. Vol. 114, Pt. 11, pp. 14,750–14,751, indicates that some Senators considered § 2511(3) as merely stating an intention not to interfere with the constitutional powers which the President might otherwise have to engage in warrantless electronic surveillance. But the Department of Justice, it was said, participated in the drafting of § 2511(3) and there is no indication in the legislative history that there was any claim or thought that the supposed powers of the President reached beyond those described in the section. In any case, it seem clear that the congressional policy of noninterference was limited to the terms of § 2511(3).

answered "No sir, we do not rely upon the affidavit itself . . . ." Tr. of Oral Arg., p. 15.[4]

Government counsel, however, seek to save their case by reference to the *in camera* exhibit submitted to the District Court to supplement the Attorney General's affidavit.[5] It is said that the exhibit includes the request for wiretap approval submitted to the Attorney General, that the request asserted the need to avert a clear and present danger to the structure and existence of the Government, and that the Attorney General endorsed his approval on the request.[6] But I am unconvinced the mere endorsement of the Attorney General on the request for approval submitted to him must be taken as the Attorney General's own opinion that the wiretap was necessary to avert a clear and present danger to the existence or structure of the Government when in an affidavit later filed in court and specifically characterizing the purposes of the interception and at least impliedly the grounds for his prior approval, the Attorney General said only that the tap was undertaken to secure intelligence thought necessary to protect against attempts to attack and subvert the structure of Government. If the Attorney General's approval of the interception is to be given a judicially cognizable meaning different from the meaning he seems to have ascribed to it in his affidavit filed in court, there obviously must be further proceedings in the District Court.

Moreover, I am reluctant myself to proceed in the first instance to examine the *in camera* material and either sustain or reject the surveillance as a necessary measure to avert the dangers referred to in § 2511(3). What Congress excepted from the warrant requirement was a surveillance which *the President* would assume responsibility for deeming an essential measure to protect against clear and present danger. No judge can satisfy this congressional requirement.

Without the necessary threshold determination, the interception is, in my opinion, contrary to the terms of the statute and subject therefore to the prohibition contained in § 2515 against the use of the fruits of the warrantless electronic surveillance as evidence at any trial.[7]

There remain two additional interrelated reasons for not reaching the constitutional issue. First, even if it were determined that the Attorney General purported to authorize an electronic surveillance for purposes exempt from the general provisions of the Act there would remain the issue whether his discretion was properly authorized. The United States concedes that the act of the Attorney General authorizing a warrantless wiretap is subject to judicial review to some extent, Brief for the United States, pp. 21–23, and it seems improvident to proceed to constitutional questions until it is determined that the Act itself does not bar the interception here in question.

---

[4] See also Transcript of Oral Argument, p. 17:

"Q. [I]f all the *in camera* document contained was what the affidavit contained, it would not comply with the Safe Streets Act?

"Mr. Mardian: I would concur in that, Your Honor."

[5] The Government appears to have shifted ground in this respect. In its initial brief to this Court, the Government quoted the Attorney General's affidavit and then said, without qualification. "These are the grounds upon which the Attorney General authorized the surveillance in the present case." Brief for the United States, p. 21. Moreover, counsel for the Government stated at oral argument "that the *in camera* submission was not intended as a justification for the authorization, but simply [as] a proof of the fact that the authorization had been granted by the Attorney General of the United States, over his own signature." Tr. of Oral Arg., pp. 6–7.

Later at oral argument, however, the Government said: "[T]he affidavit was never intended as the basis for justifying the surveillance in question . . . . The justification, and again I suggest that it is only a partial justification, is contained in the *in camera* exhibit which was submitted to Judge Keith . . . . We do not rely upon the affidavit itself but the *in camera* exhibit." Tr. of Oral Arg., at pp. 14–15. An in its reply brief, the Government says flatly: "These [*in camera*] documents, and not the affidavit, are the proper basis for determining the ground upon which the Attorney General acted." Reply Brief for the United States, p. 9.

[6] Procedures in practice at the time of the request here in issue apparently resulted in the Attorney General merely countersigning a request which asserted a need for a wiretap. We are told that under present procedures the Attorney General makes an express written finding of clear and present danger to the structure and existence of the Government before he authorizes a tap. Tr. of Oral Arg., pp. 17–18.

[7] Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefore may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter." 18 U.S.C. § 2515.

Second, and again on the assumption that the surveillance here involved fell within the exception provided by § 2511(3), no constitutional issue need be reached in this case if the fruits of the wiretap were inadmissible on statutory grounds in the criminal proceedings pending against respondent Plamondon. Section 2511(3) itself states that "[t]he contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding *only* where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power." (Emphasis added.) There has been no determination by the District Court that it would be reasonable to use the fruits of the wiretap against Plamondon or that it would be necessary to do so to implement the purposes for which the tap was authorized.

My own conclusion, again, is that as long as nonconstitutional, statutory grounds for excluding the evidence or its fruits have not been disposed of it is improvident to reach the constitutional issue.

I would thus affirm the judgment of the Court of Appeals unless the Court is prepared to reconsider the necessity for an adversary, rather than an *in camera*, hearing with respect to taint. If *in camera* proceedings are sufficient and no taint is discerned by the judge, this case is over, whatever the legality of the tap.

American Civil Liberties Union Report on the Costs and Benefits of Electronic Surveillance

(By Herman Schwartz, Professor of Law, State University of New York at Buffalo)

SUMMARY OF FINDINGS ON THE AMOUNT, BENEFITS, AND COSTS OF OFFICIAL ELECTRONIC SURVEILLANCE

I. Amount of surveillance

1. There is a vast amount of electronic surveillance, which is not covered by the figures submitted. These fall into two categories:

(a) National security (domestic and foreign);

(b) One-party consent bugging where an informant is wired for sound and police listen in.

(a) National security surveillance involves a great many taps and bugs, on many, many people, over long periods of time; the total number per year is completely unknown, so that comparisons with court-ordered eavesdropping are difficult; however, virtually every prosecution of someone whose politics are distasteful to the government seems to turn up a national security tap or bug.

(b) The one-party consent eavesdropping is perhaps the most widely used form of electronic surveillance, and unlike the national security surveillance, is used on the state as well as federal level.

2. Tens of thousands of people are reported to have been overheard by federal agents in hundreds of thousands of reported surveillances, many if not most of whom are quite innocent, not including the substantial amount of national security eavesdropping which inevitably involves a great many people per surveillance, nor the one-part consent surveillance. It is not clear that quite that many separate individuals were overheard because one cannot know from the figures whether there was any duplication so that the same person was recorded on several orders.

The totals for 1968–1970 are:

Year	Orders	Installations	People	Conversations[1]
1968	174	147	4,312	66,716
1969	302	271	31,436	173,711
1970	597	583	25,652	381,865
Total	1,073	1,001	61,400	622,292

[1] I have been informed by the Administrative Office of the U.S. Courts, which compiles and issues the figures, that an "intercept" in the report refers to a conversation.

In addition, there were an additional 171 federal installations by June 14, 1971.

The breakdown is as follows:

(a) In 1968, when there was no federal eavesdropping, state officers overheard 4312 people in 66,716 conversations in a reported figure of 147 installations.

(b) In 1969, federal officials overheard 4560 people in 44,940 conversations on 30 installed surveillances out of 33 authorizations.

State officials overheard 26,876 people in 128,171 conversations on 241 installed out of 271 authorized surveillances.

The total was 31,436 people in 173,711 conversations.

(c) In 1970, federal officers overheard 10,260 people in 147,780 conversations in 180 installations out of 183 authorizations.

State officers overheard 15,392 people in 234,085 conversations 403 installations out of 414 authorizations.

The total was 25,652 people in 381,865 conversations on 583 installations and 597 authorizations.

(d) In 1971, the projected *federal* surveillance is about 375–400 installations which at the 1970 average people and conversations per tap, may result in overhearing about 21,000 people on 300,000 conversations.

COMMENT

1. We don't know how many people and conversations were overheard in security or one-party consent eavesdropping.

2. There are some unexplained peculiarities in the figures, raising doubts as to accruacy.

3. Indeed, we know so little about how well the reporting has been monitored, and the history of self-reporting by police and other enforcement agencies is so poor, that the figures must be taken with scepticism, particularly such subjective items as "incriminating," see below.

4. Contrary to Mr. Justice Lewis Powell's statement, federal officers did not eavesdrop almost exclusively in murder, kidnapping, extortion and narcotics cases. In 1970, federal officials eavesdropped on *no* homicide or kidnapping cases and in 1969, on only *one* kidnapping case. In 1970, federal officials eavesdropped in 119 gambling cases, 40 narcotic cases, 16 credit extortion cases, and a few miscellaneous items. The state effort is also overwhelming for gambling.

II. The results of this surveillance

(a) In 1968, state eavesdropping produced *no* reported convictions, 268 arrests and 15,464 incriminating conversations out of the 4,312 people and 66,716 conversations overheard.

(b) In 1969, federal eavesdropping produced 24 convictions, 139 arrests and 36,840 incriminating conversations out of the 4,560 people and 44,940 conversations overheard.

In 1969, state eavesdropping produced 80 convictions, 486 arrests and 31,452 incriminating conversations, out of the 26,876 people and 128,771 conversations overheard.

(c) As of the report's closing date (12/31/70), in 1970 federal eavesdropping had produced 48 convictions, 613 arrests and 102,780 incriminating conversations out of the 10,260 people and 147,780 conversations overheard. An interesting breakdown is that for the 21 non-gambling and non-drug cases, the results were no convictions, 27 arrests (7 in one case related to another tap and 10 in another) and 1,193 incriminating conversations out of 1,214 people and 5,966 conversations overheard in these cases. Even in the gambling area, there were some 18 cases where no arrests were made, and where 1,760 people and 6,122 conversations were overheard, with only 215 of the conversations considered incriminating.

As of the report's date (12/31/70) in 1970, state eavesdropping produced 103 convictions, 1,261 arrests and 71,069 incriminating conversations out of the 15,392 people and 234,085 conversations overheard.

COMMENT

1. The percentage of convictions per people overheard is so small as to be virtually de minimis: In 1968, no reports; in 1969, 106 convictions out of

31,436 people overheard or about ⅓ of 1%; in 1970, as of 12/31/70, 151 convictions out of 25,652 people, or a little better than ½ of 1%. So far—and the reports are admittedly not all in yet—257 convictions reported for 61,400 people overheard, again not counting national security or one-party consent surveillance.

2. With respect to the reported convictions, we cannot know, except from self-serving Justice Department statements, whether the electronic surveillance was necessary or even helpful in the cases where it was used, even if convictions resulted—we only know that the surveillance was associated with the result.

3. Arrests are a very inadequate measure of effectiveness, since relatively few arrests ultimately produce convictions, and arrest figures are inherently unreliable.

4. The number or percentage of "incriminating" interceptions is of little to no value, since it is a highly subjective judgment and has no inherent significance. Even here, however, the percentages for non-drug, non-gambling and state cases are very low.

5. Since it seems clear that gambling and drugs cannot either be stamped out or freed from criminal entanglement merely by law enforcement techniques, is it worth allowing such a gross invasion of privacy? Indeed, all reports are to the effect that drug supplies have not substantially declined despite the increased law enforcement and electronic surveillance, and the battle against gambling has always been a failure.

III. The costs of this surveillance as reported, unreported and misreported

(a) In 1968, the state surveillance was too incompletely reported to derive useful cost figures.

(b) In 1969, federal surveillance was reported to cost $265,650 and state surveillance about $415,000, or a total of $680,650.

(c) In 1970, federal surveillance was reported to cost over $2 million, and state surveillance about $1 million, or a total of $3 million.

(d) In 1971, at the projected rate of 375–400 per year, federal surveillance will cost close to $5 million.

COMMENT

1. The above figures are grossly understated, since they omit:

(a) the large amount of national security eavesdropping;

and

(b) the vast amount of one-part consent surveillance,

and

(c) the enormous amount of man-hours by lawyers, judges and investigators to prepare applications, to keep records and to handle court challenges. The appropriate cost figure for this electronic surveillance effort may be many times the 1970 figure of $3 million.

2. There are unexplained cost differences between similar types of eavesdropping, raising questions as to accuracy of the figures. For example, FBI and Strike Force cost figures are much lower than Narcotics Bureau figures; the discrepancies on the state level are so great as to raise serious doubts about giving these figures any value.

* * * * * * *

1. National security

The national security claim is that the Executive has the right to eavesdrop electronically in order to gather intelligence about foreign and domestic groups and individuals whom the Attorney General considers dangerous, without any judicial or other check on the reasonableness of such surveillance, before it takes place, and only a minimal review if any judicial review happens to occur after. The merits of this issue will not be discussed here, but only the amount of such surveillance.

FBI Director Hoover and Attorney General Mitchell claim that the government engages in a relatively small amount of this type. For example, in April 1971, Mr. Hoover asserted that there were some 37 national security installations in operation on March 1, 1971, and Mr. Mitchell has stated that there were no more than 30 or 40.

This figure is highly misleading for it is immediately compared with the much higher number of court ordered surveillances, i.e., 180 in 1970. The

30–40 figure is misleading because it refers to the number in operation *at any* one time, in contrast with the figures for court-ordered surveillance, which are for the whole year. A check of 3 days chosen at random for court-ordered federal eavesdropping in 1970 shows far fewer than 30–40 at any one time: the figures for June 30, 1970, shows the following numbers of installation in effect, based on the figures in Table A for (1) date of installation and (2) number of days in effect:

On June 30, 1970, 8 were in operation.
On September 30, 1970, 13 were in operation.
On December 31, 1970, 0 were in operation.

These figures may be inaccurate, since the date of application may not be the date of installation, and the number of days of operation may not have been continuous; also the days chosen may be atypical. But the error is not likely to be so great as to overcome the gap between the three figures above and the 37 conceded national security surveillances. Some of these latter undoubtedly stayed in for the entire year, but other probably did not. Given the government's refusal to provide any further information, there is no way of knowing the total number of national security taps and bugs per year. All we do know is that figures supplied to Senator Edward M. Kennedy by Attorney General Mitchell indicate the federal government tapped and bugged three times as many days for national security purposes, as it did pursuant to court-order.*

A high estimate for the total number of national security eavesdropping is suggested by the fact that in virtually every prosecution of a militant, or activist dissenter a "national security" tap or bug comes to light—Benjamin Spock, the Berrigans, the White Panthers in Michigan, Abbie Hoggman and the Mayday demonstrations, the Chicago 7 trial, Black Panther prosecutions in Connecticut and California, a Weatherwoman prosecution in Buffalo, the Jewish Defense League, apparently Daniel Ellsberg, etc., etc., etc., etc., to say nothing of the known taps on Martin Luther King, Jr., Elijah Muhammad and others. The brief for the respondent in *United States* v. *U.S. District Court*, U.S. Sup. Ct., Oct. 1971 term, 70–153, the domestic security wiretap case, contains a lengthy list of such cases.

There is also reason to suspect that the "30–40 at any one time" figure is itself dubously low. As Fred Graham of the New York Times has recently shown, there is a long history of governmental duplicity in this matter. This history includes: (1) artful references in prior years by FBI Director Hoover to less than 100 wiretaps (all allegedly in "national security" cases) which carefully omitted reference to a huge number of bugs, i.e., room microphones; (2) replacement of taps by bugs to keep down the number of taps for purposes of the annual report; and (3) even assertions that some taps were disconnected the day before Mr. Hoover's testimony so that he could present a low figure as of the day he was testifying, an assertion which Mr. Hoover has, of course, indignantly denied.

One FBI agent has described Attorney General Mitchell (who authorizes these national security taps and bugs) as "a signing fool. . . . We just ask him and he signs them," (*Newsweek*, 5/10/71, p. 30A), and there is some evidence to support this implication of less than scrupulously restrained authority. For example, in the Jewish Defense League case, Mitchell certified that the JDL was tapped in connection with foreign security matters and that "it would prejudice the national interest to disclose the particular facts contained in the sealed exhibits concerning this surveillance other than to the court, *in camera*." Yet, when the Court ordered that these logs be turned over to the defendant two weeks later, the Department complied, rather than face a dismissal of the case, even though it could easily have refused and appealed, the basis for the order being a rather novel (though to this observer, correct) legal position. Indeed, in that case, it was also disclosed that whereas the government initially asserted that the tapping of the JDL stopped when the indictment came down, the surveillance actually continued well after the indictment, almost up to the day the government agreed to turn over the logs. Inevitably, lawyer-client conversations were overheard, recalling the Judith Coplon case.

---

*Senator Kennedy has not yet released the correspondence, but has publicly announced his conclusions as to the comparative time periods at a B'nai B'rith speech on October 19, 1971, and at the hearings on Supreme Court nomination of William Rehnquist.

Not only may this surveillance be very widespread, but because of the alleged desire to obtain general intelligence for preventive purposes about dangerous groups, it continues for a very long time indeed, as the JDL case showed, and as congressional testimony and experience in other cases shows. See H. Schwarts, *The Legitimation of Electronic Eavesdropping: The Politics of "Law and Order,"* 67 Mich. L. Rev. 455, 468–72 (1969). Moreover, such surveillance is especially likely to catch numerous innocent people, as all such "strategic intelligence" surveillance is admitted by the FBI to do. *Id.* at 469–70.

* * * * * * *

American Civil Liberties Union Report on the Costs and Benefits of Electronic Surveillance—1972

(by Herman Schwartz, Professor of Law, State University of New York at Buffalo)

INTRODUCTION [1]

The Electronic Eavesdropping Act has now been in operation some four and a half years. Hundreds of wiretaps and bugs have been installed, numerous court cases have been decided, millions of dollars have been spent, but the controversy over the value and dangers of electronic surveillance continues. In 1968 Richard M. Nixon promised to reverse Ramsey Clark's policies and use wiretapping to reduce crime—what kind of crime, and how that would be done, was not made clear. Four years, much money, and many crimes later, electronic surveillance is still being touted by its supporters as, in Frank Hogan's phrase, "the single most valuable weapon in the fight against organized crime." Wiretapping is given credit for major convictions in the drug area; Brooklyn District Attorney Eugene Gold promises to break the back of organized crime with his million and a half feet on a Canarsie junk yard trailer. Nevertheless, grave reservations about electronic eavesdropping continue.

One of the more useful features of the rather pourous statute pushed through in the wake of Robert Kennedy's death in 1968 by Senator John L. McClellan and his friends, is a requirement that prosecutors and judges involved in authorizing court-order wiretapping and bugging make annual reports on this surveillance which would set forth the type of surveillance (telephone tap or microphone bug), where and how long it was in operation, the crimes it was installed for, the number of people and conversations overheard, how much it cost and the results. These reports are published every May by the Administrative Office of the United States Courts. Four of these reports have been issued so far.

In the Spring of 1971, Senator McClellan announced he would hold hearings on the reports and what they showed. These have not yet been held or even scheduled; as of this writing (February 1973); one can only guess at the reasons.

The reports have nevertheless, been available, and though it is still too early to fully assess the results, certain conclusions have become clear. Some of these were published in December 1971 in report prepared by this writer for the American Civil Liberties Union on the 1968–1970 statistics. The 1971 figures became available in 1972 and it seems worthwhile to update that report, and also to add some statistical and other information that has come to light since December 1971. Again, it may still be too early for definitive conclusions—the 1972 figures available in May 1973 will be particularly useful since they will probably contain fairly complete results on the heavy federal tapping and bugging in 1970. But, as noted, certain conclusions are beginning to take shape.

The 1971 ACLU report opened with a disclaimer about the incompleteness of the reported figures, which omitted the so-called national security eavesdropping and the consent variety. Neither of these requires a court order, and thus

---

[1] This study was made possible by a grant from the Playboy Foundation. I should also like to thank Marc Chodrow, who assisted in the statistical compilation and analysis.

neither is reported to the Administrative Office. It was therefore necessary to make an educated guess at the former, with no information at all as to the latter.

Those disclaimers are still in order, particularly as to the amount of electronic surveillance involving agents wired for sound. As to these, all we have are informed guesses that this is very widely practiced on both the federal and state levels.

Thanks to data obtained and published by Senator Edward F. Kennedy, we now know something about the national security surveillance, however, and some of that will be discussed here. In addition, there have been some crucial legal developments in this area and they will also be reviewed.

This paper will consist of the following: (1) an introductory section containing a summary of the various findings, as well as certain methodological caveats and qualifications; (2) a discussion of national security surveillance; (3) a summary of the statistical data on court-authorized electronic surveillance that is contained in the annual reports from 1968–71, broken down into:

(a) The scope and variety of electronic surveillance, *e.g.*, number of installations, people and conversations overheard, length of time of overhearing, and types of offenses involved;

(b) the costs of such surveillance, both totally and broken down by offenses;

(c) the results so far in terms of convictions, arrests and incriminating conversations.

Throughout, information gleaned from the many court decisions already handed down, will be referred to where relevant; relevant information used in the 1971 report will also be worked in.

I. Summary and Methodology

A. SUMMARY

1. Amount of surveillance

a. Court-ordered.—There is a vast amount of electronic surveillance of the American people, on both the federal and state levels. A great deal of this is performed in the name of national security, and is completely uncontrolled. Much of this surveillance lasts for very long periods of time; on the state level, it is concentrated in just two states.

The bulk of this wiretapping and bugging is now used for gambling offenses, despite the original claims that it was necessary primarily for serious crimes like homicide, kidnapping and espionage: in three years, there has been only one federal device installed for kidnapping and none for either homicide or espionage; gambling installations accounted for about 90% of all the federal installations in 1971.

The figures are as follows:

	Orders	Installations	People	Conversations
1968 (6 mo.)	174	167	4,250	62,291
1969	302	290	14,656	186,229
1970	597	590	25,812	373,763
1971	816	792	32,509	496,629
Total[1]	1,889	1,839	77,227	1,118,912

[1] Combined Federal and State.

FEDERAL

In 1969–71, federal officials overheard 29,513 people in 442,157 conversations over 491 installations, as follows:

	Orders	Installations	People	Conversations
1969	33	30	4,256	41,929
1970	183	180	10,158	143,508
1971	285	281	15,099	256,720
Total	501	491	29,513	442,157

STATE

In 1968–71, state officials overheard 47,714 people in 676,755 conversations over 1,348 installations. The overwhleming bulk of this was in New York and New Jersey, with the major share in New York. To some extent, this is an estimate, but only to a very minor extent.

	Orders	Installations	People	Conversations
1968	174	167	4,250	62,291
1969	269	260	10,400	144,300
1970	414	410	15,654	230,255
1971	531	511	17,410	239,909
Total	1,388	1,348	47,714	676,755

COMMENTS

1. These figures differ somewhat from the ACLU 1971 Report because they are based on calculations derived from the reports of the individual installations and authorizations, rather than from the overall averages and summaries as in the 1971 Report.

2. Although the federal average was some 13.5 days per installations, a very high percentage of the New York installations lasted for many, many months.

3. Although the states, (which means largely New York and to a lesser extent, New Jersey) originally used the technique largely for drugs and non-gambling offenses, by 1971, the states had shifted to overwhelming concentration on gambling. Despite the pleas of need for serious offenses, the federal usage concentrated on gambling right from the start, and indeed increased that concentration at the expenses of drugs and others. The breakdowns are as follows:

	Gambling	Drugs	Homicide[1]	Kidnapping	Other
Federal installations:					
1969	20	4	0	1	5
1970	120	39	0	0	21
1971	248	21	0	0	12
Total	388	64	0	1	38
State installations:					
1968	18	68	20	1	60
1969	78	80	19	1	82
1970	204	84	20	0	95
1971	304	104	18	1	84
Total	604	336	77	3	321

[1] Includes attempts, threats, solicitations and conspiracy to commit homicide (including manslaughter) as well as a few occasional instances of consummated murder.

4. During the four year period, only 2 applications were denied, (in 1969); there is also some independent evidence of judge-shopping. For this and other reasons, there is reason to doubt that the court-ordered system is imposing meaningful controls, particularly on the state level.

b. National security.—Figures released by Senator Edward F. Kennedy indicate that at least the following number of national security wiretaps and bugs were installed:

June 12, 1968 (50 taps and 6 bugs)	56
1969 (81 taps and 13 bugs)	94
1970 (97 taps and 16 bugs)	113

1. On the basis of classified information provided the Senator, his staff has calculated that the average national security installations lasted from 78.3–209.7 days, or about 6 to 15 times the court-ordered variety of 13.5.

During 1969–71, the latter caught an average of 56 perople and 900 conversations per installation lasting an average of 13.5 days. If the court-ordered averages are roughly comparable to the national-security type—and there is no reason to think otherwise—then the 100 national security surveillances annually may well have been intercepted: From 31,000 to 84,000 people per year; from 546,000 to 1,350,000 conversations per year.

2. Electronic surveillance for domestic security purposes allegedly accounted for very little of the national security total since the Department of Justice claims it found it necessary to shut off less than 10 devices as a result of the Supreme Court's decision banning such electronic surveillance without a warrant. Thus, this vast amount of surveillance is likely to continue.

3. This known surveillance may not be all there is, since it does not include electronic surveillance by the Army (which was revealed last summer) or possible surveillance by the CIA and other agencies, or interception of teletype messages.

4. According to Ramsey Clark, such surveillance rarely produces anything of value. He has testified that if all were shut off, "the impact on our national security . . . would be absolutely zero."

2. Costs

a. Court-ordered surveillance.—The State figures are approximations, but are fairly close since the state cost reporting approached but was not equal to 100%.

	Federal	State	Tota
1968		$200,000	$200,000
1969	$440,287	470,000	910,287
1970	2,116,266	938,000	3,054,226
1971	2,114,216	1,502,340	3,616,556
Total costs	4,670,769	3,110,340	7,781,069

b. National security.—Using the same 6–15:1 time ratio of national security: court ordered surveillance as earlier, and on the premise that most of the costs are manpower costs which vary with time, one can roughly estimate the costs of an average national security installation as about 6–15 times the $9,500 of the 1969–71 federal installations, or about $47,000–$142,500 per national security installation.

Since there have been about 100 national security installations each year, a rough estimate of the annual costs of national security surveillance is from $5.7 million to $14.3 million annually.

c. Comments.—1. These figures do not include the very substantial amount of judges' and lawyers' time necessary to prepare the court-ordered applications, and the lawyers' and FBI time for the national security authorizations by the Attorney General.

2. (a) There are inexplicable differences among the different types of offenses for which federal surveillance is used, particularly between drugs on the one hand, and gambling and the other offenses on the other. Moreover, there are startling fluctuations in costs from one year to the next for, e.g., the drug surveillance: from $61,825 per installation in 1969 to $26,035 in 1970 and $12,772 in 1971. The gambling average remains relatively stable and relatively low, whereas the "Other" category drops steadily from $9,212 in 1969 to $5,794 in 1971.

(b) The state figures vary and fluctuate so greatly, that no pattern is even discernible. Thus, the gambling average rises slightly, but drugs, and Other rises very steeply, while Homicide jumps up and down and kidnapping falls sharply. These fluctuations are so inexplicable that the only conclusion is that the reports are unreliable.

3. Results

Because it takes close to two years for cases to be disposed of, at least on the federal level, the figures for convictions are still incomplete, except perhaps for 1969 convictions and the 1969–70 arrests; the incriminatory conversations are likely to be fairly complete. So far, the results seem to be as follows:

a. State.—

PERSONS CONVICTED, BY OFFENSE

	Gambling	Drugs	Homicide[1]	Kidnapping	Other	Total
1968					[2] 16	[2] 16
1969	33	32	3	0	99	167
1970	212	65	1		55	333
1971	117	55	8		30	210
Total	362	152	12	0	200	726

[1] Includes all types of homicide-related offenses, including attempts, threats, solicitation, conspiracy, manslaughter, etc.
[2] May be the result of incomplete reporting.

So far, only 194 out of the 1,448 installations have been directly associated with convictions; a small additional percentage may have been related thereto. For 1969, the year where most results are probably in, 55 out of 260 installations were associated with a conviction. As noted below, it is uncertain when and whether "associated with" involved a causal connection.

PERSONS ARRESTED, BY OFFENSE

	Gambling	Drugs	Homicide	Kidnapping	Other	Total
1968	69	97	6	7	83	262
1969	302	86	41	2	218	645
1970	930	228	19		152	1,329
1971	1,380	346	27		211	1,964
Total	1,681	757	93	9	664	4,200

These arrests are probably fairly complete for 1968–1970.

Incriminating conversations, based on prosecutors reports

	Percent incriminating
1968	22
1969	28
1970	30
1971	53

b. Federal.—

PERSONS CONVICTED, BY OFFENSE

	Gambling	Drugs	Kidnapping	Other	Total
1969	101	24	0	2	127
1970	123	99		10	232
1971	76	21		18	115
Total	300	144	0	30	474

In 1969, 12 of the 30 installations were associated with a conviction: 9/20 of the gambling installations, 2/4 Drug, and 1 out of 5 Other.

The only year for which figures seem relatively complete is 1969. The overall reported cost for this surveillance—omitting the unreported lawyers' and judges' time costs—was $440,287 or about $3,500 per person convicted, and $37,000 for each of the 12 installations with which convictions were associated.

PERSONS ARRESTED, BY OFFENSE

	Gambling	Drugs	Kidnapping	Other[1]	Total
1969	217	57		80	354
1970	730	280		26	1,036
1971	676	116		25	817
Total	1,623	453	0	131	2,207

For 1969 and 1970, the figures are probably close to complete. During this period, 92 out of 140 gambling installations were associated with an arrest, 26 out of 43 drug installations, 0 out of 1 kidnap installation, and 13 out of 26 Other, for a total of 131 out of 210 total.

INCRIMINATING CONVERSATIONS

The overall federal figures as reported are quite high: 82% in 1969, 70% in 1970 and 71% in 1971. But the non-drug and non-gambling installations produce very few incriminating conversations.

c. Comments.— 1. There is good reason to conclude that the electronic surveillance was not necessary to at least some of the convictions obtained; indeed, in some cases, courts and prosecutors found or admitted as much.

2. The arrest figures are of little significance to this issue. Not only are arrests subject to manipulation, of which there is some evidence, but wiretaps and bugs may not be installed unless there already is probable cause to arrest at least someone, and the reported court cases confirm this.

3. Much of the federal wiretapping and bugging is on small-time gamblers; Justice Department figures and reported cases so indicate. Despite claims of high value and effectiveness or organized crime, law enforcement authorities have sharply reduced their usage for every offense but gambling since 1968.

4. At least in one case a court has found that the federal government's reports of "incriminating" conversations was overstated many times. In any event (1) the definition and application of "incriminatory" is highly subjective, rarely testable, and often self-serving; (2) also, there is a good deal of evidence that very little effort to minimize non-"incriminatory" interceptions is made on the state level, and not too much more on the federal level.

5. Few of the major industrial states, which could be expected to "need" this authority, have adopted it. Indeed, most state (and much federal) wiretapping is in New York, and New Jersey, California, Illinois, Pennsylvania, Ohio and other states with major crime problems have not even bothered to give their police this authority; many states which have created such authority don't bother using it.

6. There is no indication that the heavy law-enforcement effort has substantially reduced the drug or gambling problems, or that it ever can. Causality is particularly difficult to trade for the increase in electronic surveillance has been accompanied by a very heavy increase in men and money for all other law enforcement operations.

B. SAME METHODOLOGICAL NOTES

The figures for court-authorized surveillance that are analyzed in this study are drawn from the Annual Reports issued by the Administrative Office of the United States Courts for the years 1968–71. These Reports contain data relating only to court-authorized surveillance; so-called national security and one-party consent surveillance are not done pursuant to court orders and therefore are not included in the Annual Reports. Whatever information we have as to the national security surveillance and consent eavesdropping is from other sources.

The figures in the Annual Reports on judicially authorized surveillance are broken down into three sections:

(1) Summary tables, which contain both summary figures and averages; for some reason, totals for certain categories such as total persons or conversations overheard, are not published, perhaps because the averages are based on less than the total number involved since in several instances, the prosecutor or court omitted the relevant information. The Tables are identified by numbers.

(2) An Appendix containing individual date for each installation, relating to identity of judge and prosecutor, type of offense, type and place of surveillance, length of surveillance, number of persons and conversations overheard, costs and results; these appear in the Appendix in Tables A (judge reports) and B (prosecutor reports).

(3) Follow-ups on surveillances of prior years, set out both in summary form and individually (Table C) in the Appendix.

The 1971 ACLU report depended largely on the summary tables for its overall figures. The averages were multiplied by the total number of installations

to obtain totals for persons and conversations overheard, and overall costs. For this report, an effort was made to work directly from the individual application reports in Tables A and B (and C where follow-ups were concerned) in the Appendix rather than from the summary figures in the numbered Tables at the beginning of the reports. In a few cases, there were startling and inexplicable differences between the averages and othr figures in the Administrative Office Report (hereafter referred to as "Admin. Off. Rep."), and the results from analyzing the individual installation reports in the Appendix. These discrepancies will be noted and discussed where relevant.

It should be noted that because the reporting authorities often omitted to send in important information as to persons or conversations overheard, or costs, the total figures given here are often estimates, obtained by multiplying the average for those installations that were submitted, by the total number of installations. Since full data were in fact provided for almost all federal and most state installations, the estimate seems reliable.

Certain other methodological caveats may be worth noting at this time, though they will be specifically noted where they come up. The specific offense classifications are geared to the classifications made by the Administrative Office; where there were doubts because more than one offense was indicated for an installation (as was often true for New York City authorizations) the exact classification was obtained from the Administrative Office which used a system whereby a multiple-offense authorization was classified according to the Office's judgment as to the most serious offense among those listed.

Finally, the offenses are divided into five groups: Gambling, Drugs, Homicide, Kidnapping, Other. The first two are chosen because they are the offenses for which electronic surveillance is most frequently used; Homicide and Kidnapping are the offenses for the solution of which such surveillance is most frequently said to be necessary; all the other offenses can be conveniently lumped together. "Homicide" includes every type of homicide—related offense, such as solicitation to commit homicide, attempt, conspiracy, threat and manslaughter as well as actual murders, of which there are very few instances in the Reports.

II. National Security Surveillance

The Federal Government has been using wiretapping and bugging in so-called national security cases at least since 1940, when President Franklin D. Roosevelt approved it in the interests of national defense. The FBI, which began to develop an intelligence function of major proportions at this time, in addition to its efforts in investigating particular crimes, used wiretapping and bugging quite extensively. How much we do not know, but there are indications that it was quite extensive.[2]

In the 1960's the Justice Department developed a great concern about organized crime. The FBI had apparently down-played this problem until then, but the new Attorney General, Robert F. Kennedy, went at it with truly religious zeal; the story is told in Victor Navasky's *Kennedy Justice*. There was still much uncertainty about the number of so-called "national security" taps and bugs, for the only information that was made available about this was in annual statements by Hoover before a friendly House Appropriations Committee in which he reported the number of *telephone* taps in operation *on the day he was testifying*. In a brief in the Supreme Court, in *United States* v. *U.S. Dist. Ct., E. D. Mich.*, 407 U.S. 297 (1972), the Government summarized the number of "warrantless national security telephone surveillances operated by the Federal Bureau of Investigation in the past ten years . . . [as follows]: 1960–78; 1961–90; 1962–84; 1963–95; 1964–64; 1965–44; 1966–32; 1967–38; 1968–33; 1969–49; 1970–36," citing three congressional hearings. And in 1971, President Nixon declared:

"Now in the two years that we have been in office—now get this number—the total number of taps for national security purposes by the FBI, and I know because I look not at the information but at the decisions that are made—the total number of taps is less, has been less than fifty a year."

[2] Detailed analysis of the history of national security surveillance appears in Theoharis & Meyer, *The "National Security" Justification for Electric Eavesdropping: An Elusive Exception*, 14 Wayne L. Rev. 749 (1968) Navasky & Lewin, *Electronic Surveillance* in Gillers and Watters (eds.), INVESTIGATING THE FBI (Doubleday 1973)

The figures in the Government's brief and in Nixon's statement have now been revealed to range from the disingenuously incomplete to blatantly false. Analysis of the excerpt from the Government's brief in the domestic security wiretap case, together with information obtained by Senator Edward F. Kennedy and made public in December 1971, discloses that:

(1) The figures submitted by the Government to the Supreme Court related solely to the number in operation on the day that Hoover testified—duly noted in the Government's brief in the Court of Appeals but inexplicably omitted from the Supreme Court brief;[3]

(2) The figure given by Nixon is far off the mark, despite his claim that he "look[ed] not at the information but at the decisions", whatever that means.

(3) The figures given by Nixon and in the Government's brief related solely to telephone taps installed by the FBI.

(a) They do not include microphone surveillances which, at least in the early 1960's, were as numerous as telephone taps. For example, Navasky's book contains a letter from Assistant Attorney General Herbert Miller to Senator Sam J. Ervin that on February 8, 1960, there were 78 telephone taps—the number given for 1960 by Hoover—and in addition 67 "electronic listening devices." See Kennedy Justice 88. Thus the total was really 145 on that date alone, and several times that for the whole year, if the 1969–71 figures for the relationship between the at-one-time and the annual total are an appropriate model.[4]

(b) They do not include surveillances made by *other* governmental agencies, federal and state. For example, New York Times reporter Seymour Hersh has obtained Army memoranda indicating that the Army engaged in electronic surveillance for national security purposes. (N.Y. Times, 9/1/71, p. 24, col. 1) Navasky and Lewin quote a former Justice Department official's statement that FBI "agents routinely inspired" bugs and taps by local officials. Op. cit. supra at 299–300. Moreover, they note that Hoover's testimony "leaves open the possibility (indeed informed sources within the department indicate it is a fact) that although he has neglected to mention it to Congress, Mr. Hoover is not referring to all of the taps in which the Bureau is involved. (1) He may be omitting the long-term embassy taps which were put on in the first place—some as long ago as during World War II—not at the instigation of the FBI, but of other agencies, such as the State Department, but which the FBI services. (2) He is omitting all of the taps requested by foreign intelligence agencies such as the CIA, which are not permitted to tap domestically yet have domestic intelligence needs. The FBI handles those taps and passes on the information (which it also absorbs). (3) He is omitting the interception of teletype message." Op. cit. supra at 300.

The actual totals of national security surveillances by the FBI in operation between June 1968 and December 1970, reported by the Justice Department to Senator Kennedy were as follows:

June–December 1968	(50 taps and 6 bugs)	56
1969	(81 taps and 13 bugs)	94
1970	(97 taps and 16 bugs)	113

These much higher figures are consistent with the fact that every time a war resister or dissident has been prosecuted, national security taps popped up not merely on him, but on many people subpoenaed, or in some way connected with him—see, e.g., Spock, Ellsberg, the Berrigans, Abbie Hoffman, Bradford Lyttle, Leslie Bacon, etc., to say nothing of the earlier FBI taps and bugs on Martin Luther King, Jr. and Elijah Muhammed. The defendant's brief in the domestic security wiretap case contains a list of those known to date.

On the basis of classified data supplied by the Justice Department, Senator Kennedy's staff also calculated that on the average, the 1969–70 devices were in operation from 6 to 16 times as long as the average court-approved surveillance—i.e., from 78.3 to 209.7 days, the average federal court-approved installa-

[3] Fred Graham and Navasky & Lewin have raised the possibility that these figures were understated because Hoover turned off some of the taps the day before he testified, so his statement could be superficially accurate.

[4] These probably included a certain number of organized crime surveillances, though that aspect of the FBI's eavesdropping was still minor at that time, before Robert Kennedy became Attorney General.

tion lasting about 13.5 days.[5] Since the average federal tap averaged about 56 people per interception over the period 1969–71 (491 installations and 27,299 people) or about 4 people per day of operation (56 ÷ 13) this means that from 312 to 840 people were overheard each year on each of the approximately 100 annual FBI national security subveillances, or from about 31,000 to 84,000 persons each year. Even if one discounts somewhat for duplication in people (though the 56 person average on court-authorized surveillance is supposed to be without duplication) this figure may still be conservative, since the national security surveillances were often on organizations where the telephone usage is much greater than on the private homes that were the targets of much of the court-ordered variety. For example, there were 9 telephones at the Jewsih Defense League offices that were tapped for 208 days.[6]

From these figures it is also possible to extrapolate a very rough and conservative estimate of the number of conversations overheard. Again, using the 1969–71 figures, the daily average of conversations overheard on federal 1969–71 surveillances was about 70 per installation. (The 900 average per installation divided by the 13 day average.) Since the national security taps lasted on the average from 78 to 208 days each, the number of conversations overheard annually is between 5,460 and 14,560 per installation or between 546,000 and 1,350,000 per year for the approximately 100 installations.

These figures are staggeringly high. They may actually be understated in many respects since some or many of the 100 installations may cover more than one device, as the JDL tap did, or one location. Furthermore, these figures omit the previously mentioned possibility of surveillance by other agencies, such as the Defense Department, CIA or state agencies tapping on behalf of the federal government's security programs; they omit teletype interceptions as well.

Because the whole business is so secret, we have no way of knowing the concrete results of this massive surveillance; this spying is allegedly only for intelligence purposes and not for criminal prosecution, though it seems to be around wherever there is a criminal prosecution of a noted dissident. But in congressional testimony this past June, former Attorney General Ramsey Clark testified as follows:

"I have tried to estimate—I do not know that it is possible—the value of the [national security] taps that we have. I known that not one percent of the information that we have picked up has any possible use."

And in response to a question from Senator Kennedy:

> What would be the impact on our national security if the Executive Branch were to eliminate all warrantless tapping at the present time?

Clark replied: "I think the impact would be absolutely zero." Hearings before Senate Admin. Prac. & Proc. Subcommittee on June 29, 1972, on the impact of *U.S.* v. *U.S. Dist. Ct., E. D. Mich.* 407 U.S. 297 (1972), trscpt pp. 62–63.

Last June, the Supreme Court dealt with one facet of this national security surveillance—the domestic variety. *United States* v. *U.S. Dist. Ct., E. D. Mich.*, 407 U.S. 297 (1972). In a unanimous opinion for eight members of the Court, Justice Powell writing, and Justice Rehnquist abstaining, the Court denied the Government the power to eavesdrop for purposes of domestic security without obtaining prior judicial approval, a power first openly sought in the Chicago Seven conspiracy trial and rejected by most federal lower courts. Unfortunately, the Court left open two possibilities for easy eavesdropping: (1) it virtually invited the Government to seek legislation authorizing judges to apply even looser standards for domestic security wiretapping than the already less-than-demanding standards of Title III; (2) it explicitly limited its decision to "domestic aspects of national security," and to "domestic organizations," defined as a group of American citizens "which has no significant connection

---

[5] The figure is likely to be closer to the upper part of the range. Not only was the Jewish Defense League tap in for 208 days, but of the six domestic security taps turned off as the result of the *Keith* decision, (*U.S. U.S. Ct.*) one was operated for 21 months, two for 18 months, one for 4½ months, one for 3 months, and one for 2 weeks. See letter from Deputy Asst. Atty. Gen. K. Maroney to the Kennedy Committee dated 8/2/72.

[6] That the figure is none too high is clear if one reflects for a moment on one's own business phone calls: it is more than possible to talk to more than 4 new people per day, especially if one includes both incoming and outgoing calls.

with a foreign power, its agent or agencies." (n. 11) The Justice Department's narrow construction of this latter category can be seen from the facts that: (a) Justice felt constrained to turn off very few installations as a result of the decision, and apparently left a couple in operation, N.Y. Times, 6/30/72, p. 17, col. 2; (b) it installed a tap on the Jewish Defense League and kept it in operation for 208 days [7]—including a month *after* indictment—on the asserted justification that this tapping was for national security purposes; and (c) a conversation by one of Daniel Ellsberg's lawyers was overheard on a foreign national security tap even though, as Justice Douglas disclosed with some surprise, the tap was on the phone of a foreign national, and not on a foreign agency or in any other discernible way connected with national security. *Russo* v. *Byrne*, 409 U.S. ——, 93 S. Ct. 433 (1972).

When the Army was caught in its massive surveillance program, it agreed to cleanse its files. The Department of Justice told Senator Kennedy's committee that virtually no effort had been made to cleanse the FBI files of information obtained by this illegal wiretapping and bugging. Furthermore, since at least some of it had been disseminated to state agencies without disclosing to them the source of this information, cleaning of the state files is probably impossible. From all indications, nobody has ever tried.

A great deal of electronic eavesdropping for security purposes has taken place and will probably continue; such surveillance catches a great number of people in an enormous number of conversations. Because this eavesdropping is not usually aimed at criminal prosecution, it will rarely come to light—and that is probably as intended by the Executive. The only hope for some kind of oversight is from Congress. Unfortunately, this particular Administration has succeeded beyond any other in denying information to Congress. The result, however, is that except for the summary statistics obtained by Senator Kennedy, we are not likely to obtain very much more; as a matter of fact, virtually all of Senator Kennedy's questions that sought information beyond the overall annual totals went unanswered.

TITLE 18.—UNITED STATES CODE

SECTIONS 2511–2520

§ *2511. Interception and disclosure of wire or oral communications prohibited*

(1) Except as otherwise specifically provided in this chapter any person who—

(a) willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire or oral communication;

(b) willfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) willfully discloses, or endeavors to disclose, to any other person the contents of any wire or oral communications, knowing or having reason to know

---

[7] Other long-term surveillance has come to light in national security cases. The Government's brief in the Supreme Court described the tap in a companion case as lasting 14 months. See also 22n.

that the information was obtained through the interception of a wire or oral communication in violation of this subsection; or

(d) willfully uses, or endeavors to use, the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this subsection;

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchborad, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication: *Provided*, That said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) It shall not be unlawful under this chapter for an officer, employee, or agent of any communication common carrier to provide information, facilities, or technical assistance to an investigative or law enforcement officer who, pursuant to this chapter, is authorized to intercept a wire or oral communication.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire or oral communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State or for the purpose of committing any other injurious act.

(3) Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.

§ *2512. Manufacture, distribution, possession, and advertising of wire or oral communication intercepting devices prohibited*

(1) Except as otherwise specifically provided in this chapter, any person who willfully—

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such

device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication any advertisement of—

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire or oral communications,

knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commence.

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for—

(a) a communications common carrier or an officer, agent, or employee of, or a person under contract with, a communications common carrier, in the normal course of the communications common carrier's business, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications.

§ *2513. Confiscation of wire or oral communication intercepting devices*

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

§ *2514. Immunity of witnesses*

Whenever in the judgment of a United States attorney the testimony of any witness, or the production of books, papers, or other evidence by any witness, in any case or proceeding before any grand jury or court of the United States involving any violation of this chapter or any of the offenses enumerated in section 2516, or any conspiracy to violate this chapter or any of the offenses enumerated in section 2516 is necessary to the public interest, such United States attorney, upon the approval of the Attorney General, shall make application to the court that the witness shall be instruced to testify or produce evidence subject to the provisions of this section, and upon order of the court such witness shall not be excused from testifying or from producing books, papers, or other evidence on the ground that the testimony or evidence required of him may tend to incriminate him or subject him to a penalty or forfeiture. No such witness shall be prosecuted or subjected to any penalty or

forfeiture for or on account of any transaction, matter or thing concerning which he is compelled, after having claimed his privilege against self-incrimination, to testify or produce evidence, nor shall testimony so compelled be used as evidence in any criminal proceeding (except in a proceeding described in the next sentence) against him in any court. No witness shall be exempt under this section from prosecution for perjury or contempt committed while giving testimony or producing evidence under compulsion as provided in this section.

REPEAL

Pub. L. 91–452, Title II, §§ 227(a), 260, Oct. 15, 1970, 84 Stat. 930, 931, repealed this section effective four years following the sixtieth day after the date of the enactment of Pub.L. 91–452, which was approved Oct. 15, 1970, with such repeal not to affect any immunity to which any individual is entitled hereunder by reason of any testimony or other information given before such day. See section 260 of Pub.L. 91–452, set out as a note under section 6001 of this title.

§ 2515. Prohibition of use as evidence of intercepted wire or oral communications

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

§ 2516. Authorization for interception of wire or oral communications

(1) The Attorney General, or any Assistant Attorney General specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception or wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—

(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relating to sabotage), chapter 115 (relating to treason), or chapter 102 (relating to riots);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h) or (i) of section 844 (unlawful use of explosives), section 1084 (transmission of wagering information), section 1503 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1751 (Presidential assassinations, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), sections 2314 and 2315 (interstate transportation of stolen property), section 1963 (violations with respect to racketeer influenced and corrupt organizations or section 351 (violations with respect to congressional assassination, kidnapping and assault);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving bankruptcy fraud or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under section 892, 893, or 894 of this title; or

(g) any conspiracy to commit any of the foregoing offenses.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire or oral communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire or oral communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

§ 2517. *Authorization for disclosure and use of intercepted wire or oral communications*

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire or oral communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire or oral communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose it privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire or oral communications in the manner authorized herein, intercepts wire or oral communications relating to offenses other than those specified in the order of authorization or approval, the contests thereof, and evidenced derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

§ 2518. *Procedure for interception of wire or oral communications*

(1) Each application for an order authorizing or approving the interception of a wire or oral communication shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire or oral communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the applications is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire or oral communications within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) there is probable cause for belief that the facilities from which, or the place where, the wire or oral communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire or oral communication shall specify—

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire or oral communication shall, upon request of the applicant, direct that a communication common carrier, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such carrier, landlord, custodian, or person is according the person whose communications are to be intercepted. Any communication common car-

rier, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefore by the applicant at the prevailing rates.

(5) No order entered uner this section may authorize or approve the interception of any wire or oral communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General or by the principal prosecuting attorney of any State or subdivision therof acting pursuant to a statute of that State, who reasonably determines that—

(a) an emergency situation exists with respect to conspiratorial activities characteristic of organized crime that requires a wire or oral communication to be intercepted before an order authorizing such interception can with due diligence be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire or oral communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire or oral communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8) (a) The contents of any wire or oral communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire or oral communication under this subsection shall be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire or oral communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7) (b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, and inventory which shall include notice of—

(1) the fact of the entry of the order of the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire or oral communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any intercepted wire or oral communication or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10) (a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any intercepted wire or oral communication, or evidence derived therefrom, on the grounds that—

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the intrests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

§ 2519. Reports concerning intercepted wire or oral communications

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for;

(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension of an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts—

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, and (iv) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire or oral communications and the number of orders and extensions granted or denied during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

§ 2520. Recovery of civil damages authorized

Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications, and (2) be entitled to recover from any such person—

(a) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;

(b) punitive damages; and

(c) a reasonable attorney's fee and other litigation costs reasonably incurred.

A good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under this chapter or under any other law.

June 19, 1972 Press Release (Except of the Attorney General)

Attorney General Richard G. Kleindienst issued the following statement today:

In accordance with the decision of the Supreme Court, I have today directed the termination of all electronic surveillance in cases involved domestic security that conflict with the Court's opinion.

Hereafter, surveillance will be undertaken in domestic security cases only under procedures that comply with the Court's opinion.

The Court invited Congress to legislate the standards and procedures for court-approved electronic surveillance in such cases—as Congress already has done in criminal cases.

Therefore, I am also directing the appropriate officers of the Department of Justice to work closely with Congress in formulating legislative standards for domestic security surveillance.

It should be noted that the Court's opinion was confined to the narrow issue of the use of electronic surveillance in domestic security cases, and it does not affect the use of electronic surveillance for the gathering of foreign intelligence in national security matters.

The Internal Security Division is reviewing pending cases to determine the effect of the opinion and will make recommendations to me on whether to disclose information obtained by electronic surveillance to defendants or to dismiss the charges against them.

○