

Y 4
.J 89/2
96-47

1042

96/4
J 89/2
47-96

WIRETAP AMENDMENTS

GOVERNMENT

DOCUMENTS

Storage

APR 30 1980

PARRELL LIBRARY
KANSAS STATE UNIVERSITY

HEARING

BEFORE THE

COMMITTEE ON CRIMINAL JUSTICE

OF THE

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

NINETY-SIXTH CONGRESS

SECOND SESSION

ON

S. 1717

A BILL TO AMEND TITLE III OF THE OMNIBUS CRIME CONTROL
AND SAFE STREETS ACT OF 1968

MARCH 5, 1980

Serial No. 96-47

Printed for the use of the Committee on the Judiciary



U.S. GOVERNMENT PRINTING OFFICE

WASHINGTON : 1980

59-967 O

COMMITTEE ON THE JUDICIARY

EDWARD M. KENNEDY, Massachusetts, *Chairman*

BIRCH BAYH, Indiana

ROBERT C. BYRD, West Virginia

JOSEPH R. BIDEN, Jr., Delaware

JOHN C. CULVER, Iowa

HOWARD M. METZENBAUM, Ohio

DENNIS DeCONCINI, Arizona

PATRICK J. LEAHY, Vermont

MAX BAUCUS, Montana

HOWELL HEFLIN, Alabama

STROM THURMOND, South Carolina

CHARLES McC. MATHIAS, Jr., Maryland

PAUL LAXALT, Nevada

ORRIN G. HATCH, Utah

ROBERT DOLE, Kansas

THAD COCHRAN, Mississippi

ALAN K. SIMPSON, Wyoming

STEPHEN BREYER, *Chief Counsel*

EMORY SNEEDEN, *Minority Chief Counsel*

SUBCOMMITTEE ON CRIMINAL JUSTICE

JOSEPH R. BIDEN, Jr., Delaware, *Chairman*

EDWARD M. KENNEDY, Massachusetts

JOHN C. CULVER, Iowa

DENNIS DeCONCINI, Arizona

PATRICK J. LEAHY, Vermont

CHARLES McC. MATHIAS, Jr., Maryland

THAD COCHRAN, Mississippi

PAUL LAXALT, Nevada

ORRIN G. HATCH, Utah

MARK GITENSTEIN, *Chief Counsel*

KATHY ZEBROWSKI, *Counsel*

HARRY WILES, *Counsel*

MICHAEL KLIPPER, *Minority Counsel*

CONTENTS

WEDNESDAY, MARCH 5, 1980

TESTIMONY

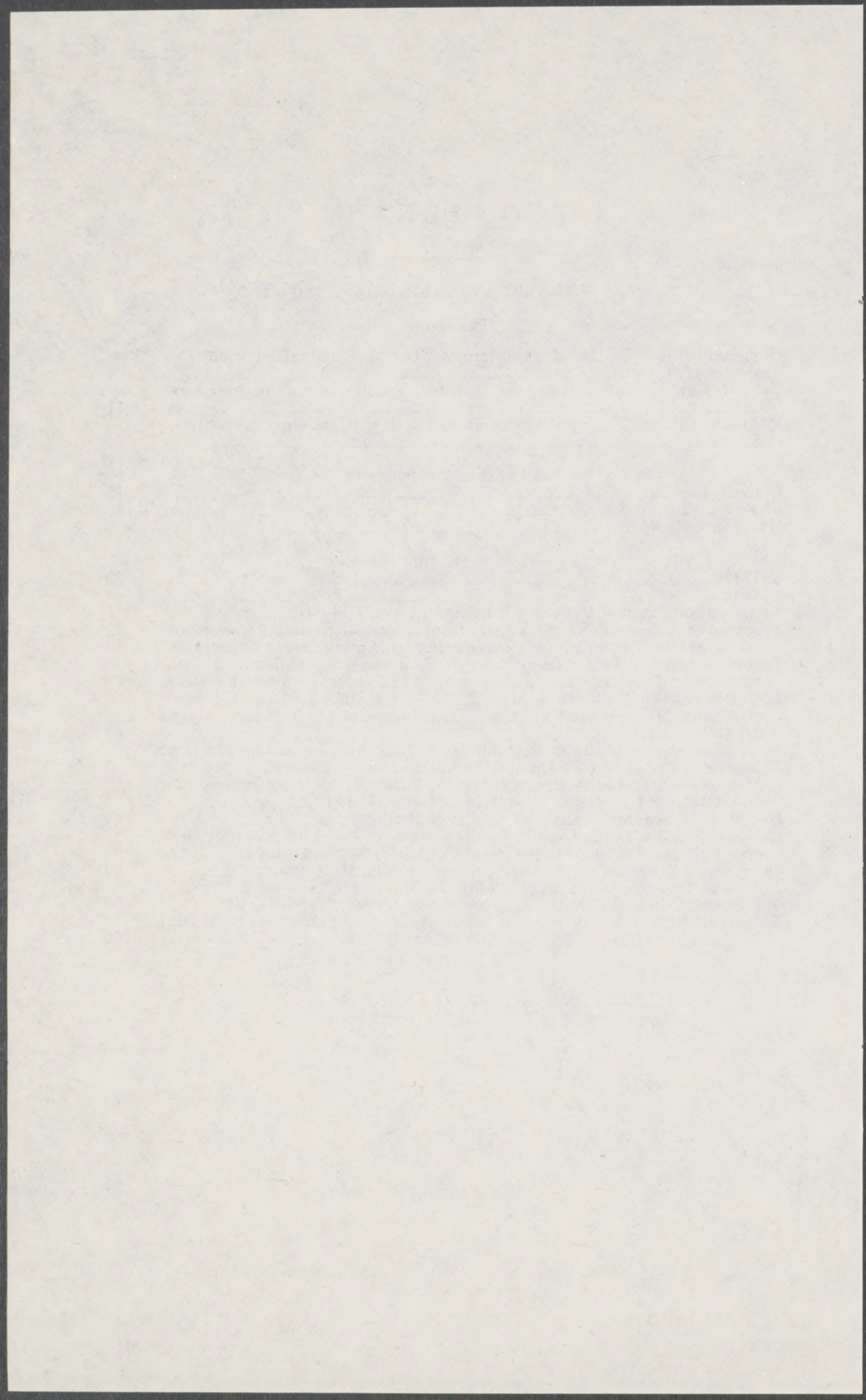
Heymann, Philip B., Assistant Attorney General, Criminal Division, Department of Justice.....	Page 4
Colwell, Lee, Executive Assistant Director, Federal Bureau of Investigation.....	11
Fishman, Clifford S., associate professor of law, Catholic University of America.....	24

PREPARED STATEMENTS

Colwell, Lee.....	15
Fishman, Clifford S.....	28
Heymann, Philip B.....	7

APPENDIX

S. 1717.....	39
S. 1815.....	44
Prepared statement of H. Stuart Knight, Director, U.S. Secret Service.....	47
Prepared statement of Kenneth J. Hodson, chairman, Standing Committee on Association Standards for Criminal Justice, American Bar Association.....	49
Letter to Senator Leahy from Peter B. Bensinger, Administrator, Drug Enforcement Administration, Department of Justice, February 29, 1980.....	60
Letter to Senator Leahy from Miles N. Keathley, Acting Director, Bureau of Alcohol, Tobacco and Firearms, Department of the Treasury, March 21, 1980.....	63
Letter to Senator Leahy from John H. F. Shattuck, legislative director, American Civil Liberties Union (Washington office), March 26, 1980.....	65
Letter to Senator Leahy from Clifford S. Fishman, associate professor of law, Catholic University of America, March 18, 1980.....	68
Questions of Senator Leahy and responses of Clifford S. Fishman.....	69
Letter to Senator Leahy from Philip B. Heymann, Assistant Attorney General, Criminal Division, Department of Justice, March 31, 1980.....	88
Questions of Senator Leahy and responses of Philip B. Heymann.....	89
Letter to Senator Biden from Philip B. Heymann, Assistant Attorney General, Criminal Division, Department of Justice, March 31, 1980.....	98
Letter to Senator Kennedy from James A. McCafferty, chief, Statistical Analysis and Reports Division, Administrative Office of the U.S. Courts.....	100



WIRETAP AMENDMENTS

WEDNESDAY, MARCH 5, 1980

U.S. SENATE,
SUBCOMMITTEE ON CRIMINAL JUSTICE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The committee met at 8 a.m., in room 2228 of the Dirksen Senate Office Building, Senator Leahy presiding.

Present: Senator Leahy.

Also present: Harry Wiles, Robert McNamara, Jr., Kathy Zebrowski, Michael Klipper.

Senator LEAHY. This session of the Judiciary Committee will be in order, and I will have first a statement from our chairman, Senator Kennedy, and this is, of course, the Subcommittee on Criminal Justice. Without objection, the chairman's statement will be made part of the record.

[The prepared statement of Senator Kennedy follows:]

PREPARED STATEMENT OF SENATOR KENNEDY

Mr. Chairman, I appreciate this opportunity to submit a prepared statement on S. 1717, legislation which would amend Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. 2510 et seq.). I regret that I am unable to appear personally before this subcommittee to discuss with you the provisions of this important legislation. I wish to commend you for your interest in this legislation as well as other legislation which directly affects the continued vitality of the criminal justice system. Your efforts to enhance the effectiveness of Federal law enforcement while at the same time guarding against erosion of the constitutional and privacy rights of our citizens are well known and admired. This legislation is another example of that effort to balance the legitimate and proper law enforcement function with the genuine concerns for privacy and individual rights.

S. 1717 addresses two distinct issues which arise in connection with the interception of wire and oral communications for law enforcement purposes: the use of surreptitious or covert entries to effect an interception under Title III and the need for authority to conduct emergency interceptions without prior court approval in situations which involve an immediate danger of death or serious physical injury to a person.

The provisions of this bill which deal with surreptitious entries are designed to provide safeguards which will insure informed judicial consideration of the need for and the reasonableness of the surreptitious entry as well as require specific court authorization for any such

entry. Title II does not now contain such safeguards, and the Supreme Court recently held in *Dalia v. United States*, 441 U.S. 238 (1979), that such safeguards are not constitutionally mandated.

The rationale of the Court in *Dalia* was, in part, based on a finding that authorization for a surreptitious entry is implicit in an order authorizing the interception of oral communications. However, the Court noted that the "preferable approach" in such cases was for Government agents to make explicit to the authorizing court their expectation that some form of surreptitious entry would be required to accomplish the interception. The Department of Justice, to its great credit, has had such a policy for a number of years which the Supreme Court noted with approval. Not only do current Department of Justice guidelines require its officers to inform the court of the need for, and to request the use of, a surreptitious entry in an application for a Title III interception when such an entry is required to execute the court order, but also the Department's model form for a Title III intercept order includes a provision specifically authorizing such an entry.

The National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance has recommended that Title III be amended to provide for specific court authorization of surreptitious entries, and President Carter strongly endorsed this recommendation in his privacy message last year. My support for such an amendment is based upon the conviction that requiring court authorization of surreptitious entries under Title III is a sound policy that will limit unnecessary encroachments on individual privacy. The power of a Government agent to enter a home or office surreptitiously lends itself to dangerous abuse and must be carefully circumscribed.

Although the Fourth Amendment does not generally require a judge, when issuing a warrant to scrutinize or specifically authorize the particular means by which the warrant is to be executed, I believe that the use of surreptitious entry to effect a Title III interception presents unique privacy considerations that merit such judicial involvement. First, the use of electronic surveillance in itself is quite correctly viewed as one of the most intrusive means of obtaining evidence of a crime. The stringent procedural requirements set forth in Title III reflect the seriousness of the breach of privacy that results from the interception of personal communications. Second, unlike the execution of a search warrant, the execution of an interception order and any attendant physical entry must be accomplished in secrecy, and thus there is no contemporaneous notice to the occupants of the premises that a breach of their privacy has taken place. Third, where covert entry occurs in the course of electronic surveillance, there is a dual encroachment on the individual's right to privacy for not only is his conversational privacy violated but his physical privacy is breached as well.

S. 1717 addresses the unique privacy concerns which arise when a surreptitious entry is used to execute an intercept order under Title III. It is not the purpose of these amendments to preclude the use of surreptitious entries for at times they are the only practical means of installing a court-authorized surveillance device which will produce evidence of a serious crime. Rather these amendments would subject such entries to the scrutiny and approval of an informed, neutral judicial officer.

A second and equally important purpose of this legislation is to provide statutory authority for an emergency interception of wire and

oral communications in life-endangering situations. It has long been recognized that exigent circumstances justify conducting a warrantless search, and this same principle should apply to the interception of wire and oral communications. Where an interception would be authorized under Title III if there were time to obtain a court order, and where such an interception could be instrumental in preventing death or serious injury, as in a kidnapping or hostage situation, a law enforcement officer should have at his immediate disposal this valuable investigative tool.

Title III does not now permit an emergency interception in life-endangering situations. It does, however, permit such interceptions in an emergency situation which relates to "conspiratorial activities threatening the national security" and "conspiratorial activities characteristic of organized crime." The exigency of an immediate threat to human life is at least as, if not a more important reason for an emergency exception.

In closing, Mr. Chairman, I would like to point out the significant contribution made by Assistant Attorney General Philip B. Heymann and his staff and Director William H. Webster and his staff with whom I worked closely in drafting this legislation. Their sensitivity to and concern for the need to protect personal privacy in the context of enhancing legitimate law enforcement efforts are the reason this legislation has such broad support.

Senator LEAHY. I should note, though, in that statement that Senator Kennedy ends with this paragraph:

In closing, I would like to point out the significant contribution made by Assistant Attorney General Philip Heymann and his staff and Director William H. Webster and his staff with whom I worked closely in drafting this legislation. Their sensitivity to and concern for the need to protect personal privacy in the context of enhancing legitimate law enforcement efforts are the reason this legislation has such broad support.

This morning we will consider S. 1717 which amends Title III of the Omnibus Crime Control and Safe Streets Act of 1968 in two significant respects: It establishes procedures for court approval of surreptitious entries and provides the new emergency exceptions for life-endangering situations.

Nearly a year ago the Supreme Court in *Dalia v. United States* held that surreptitious and covert entries performed for the purpose of installing court authorized electronic bugging equipment were not prohibited by the Fourth Amendment. The Court went on to hold that the authority for such entries was implicit in Title III intercept order and the issuing judge need not specifically authorize such entries in his order. The Court noted that the Department of Justice has for some time included a specific entry provision in its Title III application, and the Court stated that this was the "preferable approach."

This comment echoed the recommendation of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, that such entries be expressly authorized by a court order. This recommendation and legislation we are considering today has been strongly endorsed by the President and the Department of Justice.

S. 1717, which was introduced by Senator Kennedy last fall, sets forth procedures to be followed when law enforcement officers determine that a surreptitious or covert entry will be necessary to install

an electronic intercept device on a private premises pursuant to a court order. These procedures reasonably balance the legitimate law enforcement need for such entries with a social interest to protect the privacy of its citizens.

S. 1717 further amends Title III by providing a new emergency exception for a life endangering situation. Under current law, communications can be intercepted prior to obtaining a court order if an emergency situation exists with respect to conspiratorial activities which either threaten the national security or are characteristic of organized crime. These exceptions, however, fail to take into account situations where there is an immediate threat of death or serious bodily injury to persons, for example, in the case of hostage situations. S. 1717 resolves this problem by providing for such emergencies.

During the course of today's hearing, the subcommittee will discuss provisions of S. 1717 with representatives of the Department of Justice and the Federal Bureau of Investigation. We have also invited comments from other Federal law enforcement agencies, including the U.S. Secret Service, Department of Treasury, and the Drug Enforcement Administration, both from the American Bar Association and the American Civil Liberties Union. These agencies and groups which support this legislation have been asked to submit statements which will be made part of the hearing record.

We are glad to have the Attorney General of the Criminal Division here who is becoming in some ways a resident of Capitol Hill, a day-time resident of Capitol Hill. I am glad to have you here this morning, General. Please go ahead with your statement any way you like.

**STATEMENT OF PHILIP B. HEYMANN, ASSISTANT ATTORNEY
GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE**

Mr. HEYMANN. Thank you very much, Senator Leahy.

I think you and Senator Kennedy deserve a great deal of credit for this bill. I believe it is not controversial and serves only healthy and good purposes both in terms of civil liberties and in terms of protection of the public.

If my full statement can be introduced into the record, I will summarize briefly.

As you mentioned, S. 1717 addresses two entirely distinct, but equally important issues. The first is the use of surreptitious entries; the other is the availability of an exception for certain emergency life-endangering situations, particularly hostage situations as you mentioned.

Let me discuss each of these points quite briefly, one at a time.

First, surreptitious entry: the amendments proposed in S. 1717 would require that the application for an order authorizing the interception of communications state whether surreptitious entry will be required to effect interceptions, and if so, why other means of effecting the interception wouldn't do.

It requires the issuing judge to make a finding that the surreptitious entry is necessary, and it requires that the order approving the interceptions specifically state whether surreptitious entry for the purpose of effecting the interception is authorized.

Presently Title III does not contain those requirements as I understand the Supreme Court's decision in the *Dalia* case, we are all right under Title III without such an order, but our present practice, and we think the preferred practice, is consistent with what S. 1717 would require.

It is the Department's policy that where it is anticipated that surreptitious entry will be necessary, the application for a court order is to request specific authority for that entry.

As Senator Kennedy pointed out in his remarks in introducing the bill, although the Fourth Amendment generally does not require judicial approval of the particular means by which a search warrant is executed, the use of surreptitious entry in the context of electronic surveillance presents unusual, unique privacy considerations which render judicial involvement proper.

There is no way that we can do wholly without bugs or microphones. We could, but it would be extremely costly. Congress has not moved to preclude the use of microphones for a very long period of time. Bugs have been authorized since 1968 by statute, and in general, placing a microphone is going to require a surreptitious entry.

The approach of S. 1717 to regularize procedures concerning such entries through a court process seems to me to be exactly the right way to handle this situation.

The term "surreptitious entry" is defined in the bill to include entry by ruse as well as entry by force or lock-picking. That seems to us also to be correct.

I think it is important for the subcommittee to realize, as I am sure it does, and to reflect in the legislative history that in the overwhelming majority of cases the placing of a microphone is likely to require surreptitious entry which is defined broadly so as to include either a physical entry—lock picking, a breaking of a door—or entry by ruse.

It is important to note that in the legislative history because we want judges who are asked to make a specific finding that surreptitious entry is necessary to know that that is not going to be an exceptional course with regard to microphone electronic surveillance, but is going to be the general rule.

We don't mind exploring each alternative, but we would not like judges to be surprised that entry either by ruse or in some other surreptitious way is necessary to place a microphone in a closed, locked room or building.

Senator LEAHY. In fact, electronic eavesdropping by definition means you are going to be active in an area where you will be unable to enter by permission. However, if it requires a court order to get the microphones in place, or whatever other device you use, it is apparent that you will need to employ some kind of unauthorized entry.

Mr. HEYMANN. I had a hard time imagining what would be left out.

Senator LEAHY. The same here.

Mr. HEYMANN. I went over the section-by-section analysis, and the staff was quite ingenious in thinking of other ways of entry which are not surreptitious entries. Senator Leahy, they would include, for example, if a roommate or another occupant of the space said, "Sure, come on in and place a microphone."

There, there would be no problem about the entry, but the microphone would still require title III permission. There might be a few such cases.

The point that you and I are making is that in most cases, there has to be a surreptitious entry.

The only other provision that concerns us at all, I believe, on the question of court orders for surreptitious entries is the provision in section 4(g) which requires that written notice be given to the issuing judge of the time and method of the initial entry and of any subsequent entries.

The section-by-section analysis goes rather far there, too, in making it clear that a general description of the type of entry will be adequate.

I know that Mr. Colwell will talk about the difficulties of knowing in advance exactly how an entry will be made, but we are also concerned that the very precise specifics of how an entry is made not have to be laid out on a public record.

Now, out of some instinct of caution, I have never myself asked the FBI how they do an entry to place a microphone. I trust that I would be told if asked, but I have always thought that this is something that should be kept relatively closely guarded, both for the safety of the officer and for the effectiveness of the operation.

Our only concern is, once again, and perhaps the legislative history under section 4(g) could make it clear as the section-by-section analysis suggests, that you are only looking for a broad description of how the entry would be made for example, by ruse or by whatever might be the alternative of opening a window, but in some kind of general way.

Senator LEAHY. At the same time, we want it to be clear we are not authorizing a carte blanche fishing expedition—I agree with you. It does not make too much difference whether the entry is through a window or through the door or someone dressing like Santa Claus down the chimney. It isn't necessary for that specificity to be included. It must be drafted in such a way that there are parameters within which law enforcement agencies can legitimately exercise. Based on past history I think we have in the law enforcement agencies, especially the FBI, who understand those bounds beyond which they cannot go with propriety.

I am trying to determine the exact way it will go. It does not leave the kind of flexibility that protects everybody, physically protects them.

Mr. HEYMANN. In general, we always have considerably less difficulty with advising a judge orally of a matter than in spelling it out on a public record, or revealing it routinely to defendants whose interests are frequently, if not always, hostile to law enforcement. I think there is room for working out whatever concerns there are there.

If I may, I would like to turn just for a minute to the Emergency Life Endangering Amendment, S. 1717. I know that the Attorney General has approved emergency wiretaps without court order followed 48 hours later by a court order in situations concerning hostages or other grave danger.

I think that has been true of Attorneys General for a period of time. They have done it with some stretching, both of conscience and of statutory language. It has seemed entirely clear to them and to me

that Congress did not intend in Title III to preclude the temporary placing of an electronic monitoring device or of a wiretap in a situation where a bank robber was holding five people hostage or a kidnaper was taking a kidnap victim away in a car.

We have reached that conclusion through a variety of arguments; three in particular. First is through some stretch of the language on conspiratorial activities characteristic of organized crime. That is the present explicit authority Title III.

We have read taking hostages in a bank robbery or a bank robbery as conspiratorial activity characteristic of organized crime, though that is less than 100 percent clear, at best.

Second, we have found in a number of circumstances, I think quite correctly, that there is no reasonable expectation of privacy for a hostage taker in a bank or for a kidnaper in somebody else's car, and that has allowed us to place with microphone devices, despite the limited emergency provision of present Title III.

Finally, and as a third basis, I believe it is, indeed, the view of the Office of Legal Counsel in the Justice Department, that there is implicit in the statute itself, some kind of ability to save life.

Having said all that, it is plainly unwise to have Title III, which together with the Foreign Intelligence Surveillance Act is intended to cover the waterfront of electronic surveillance, leave one category of exceptions, and a category so important in its lifesaving capacity that everybody wants it, and a matter of common law and the merciful instincts of Attorneys General.

What this provision in S. 1717 would do would be simply to regularize this procedure. It would establish an emergency exception in the very situation, I think almost the exclusive situation where we now make emergency authorizations.

I don't think we are using emergency wiretap authority in any other situation. Or if we are, it is very rare. We are using it primarily only for life-endangering situations.

The proposal in S. 1717 would regularize this process, and I think it is enough to say that I think everybody would welcome that. It is really not so much a triumph not for life saving, because we will always do all we can do to preserve life, but for the rule of law it will order and regularize.

Thank you, Mr. Chairman.

[The prepared statement of Assistant Attorney General Philip B. Heymann follows:]

PREPARED STATEMENT OF PHILIP B. HEYMANN

Senator Leahy and members of the Subcommittee, I am pleased to appear before the Subcommittee to present the views of the Department of Justice on S. 1717, a bill introduced by Senator Kennedy which would amend title III of the Omnibus Crime Control and Safe Streets Act of 1968, the statute which governs the interception of wire and oral communications by federal law enforcement. The Department of Justice worked with Senator Kennedy's staff in developing this bill, and I am glad to have this opportunity to comment on its provisions.

S. 1717 addresses two distinct but equally important issues that have arisen in the context of the interception of private communications. The first is the question of the use of surreptitious entry to effect such interceptions. The second is the need to intercept communications in emergency, life endangering situations where the exigency of the situation precludes obtaining prior judicial approval. Presently, title III does not adequately meet these situations, and thus S. 1717 would

make needed improvements which are fully supported by the Department of Justice.

I shall direct my comments first to the surreptitious entry provisions of the bill and then turn to section five of the bill which concerns the emergency authorization of electronic surveillance in cases of imminent danger to human life.

SURREPTITIOUS ENTRY

The surreptitious entry provisions of S. 1717 would provide important safeguards to assure that such methods are employed by law enforcement officers executing an order permitting electronic surveillance only when such methods have been found reasonable and necessary by an informed, impartial judicial officer. Briefly, these amendments would require (1) that the application for an order authorizing the interception of communications state whether surreptitious entry will be required to effect the interception and, if so, why other means of effecting the interception are not believed to be feasible, (2) that the issuing judge make a finding that such entry appears necessary under the circumstances, and (3) that the order approving the interception specifically state whether surreptitious entry for the purpose of effecting the interception is authorized.

Title III presently does not contain any such requirements. Nonetheless, it is Department policy that where it is anticipated that a surreptitious entry will be necessary to install, maintain, or remove an interception device, the application for a court order authorizing the interception is to state that the use of such entry is expected, and specific authorization for such entry is to be included in court's order. We have not found these procedures to be burdensome. Instead, they embody what I believe to be a sensible policy which should be directly incorporated into the provisions of title III.

The adoption of such procedures was recommended by the National Commission for the Review of State and Federal Laws Relating to Wiretapping and Electronic Surveillance which was charged by Congress to study and evaluate the effectiveness of title III. The President endorsed this recommendation in his message to Congress of April 3, 1979.

It should be acknowledged that the National Commission's recommendation was based in no small part on the view that Title III was ambiguous on the issue of whether specific court authorization of surreptitious entry was required. At that time, the courts of appeals had given conflicting answers to this question. This legal ambiguity, however, was resolved by the Supreme Court's recent decision in *Dalia v. United States*, 441 U.S. 238 (1979), in which the Court held (1) that Congress in enacting title III intended to authorize the courts "to approve electronic surveillance without limitation on the means necessary to its accomplishment so long as they are reasonable under the circumstances",¹ and (2) that "the Fourth Amendment does not require that a Title II electronic surveillance order include a specific authorization to enter covertly the premises described in the order".² However, the Court noted that the "preferable approach" was for government agents to make explicit to the court their expectation that surreptitious entry would be required to effect the interception, and it cited the current Department of Justice policy to this effect with approval.³

Although the *Dalia* decision settled any question about the present legal necessity of obtaining specific court authorization to employ surreptitious entry in executing an interception order, the administration, recognizing the particularly intrusive nature of such entries and the resultant need for judicial consideration of their appropriateness in effecting electronic surveillance, recommended that title III be amended to require specific court approval of such covert entries.

As Senator Kennedy pointed out in his remarks in introducing this bill, although the Fourth Amendment generally does not require judicial approval of the particular means by which a search warrant is executed, the use of surreptitious entry in the context of electronic surveillance presents unique privacy considerations which render judicial involvement proper: first, the interception of private communications is one of the most intrusive investigative tools available to law enforcement and as such is subject to a series of procedural safeguards mandated by title III; second, physical entries in the context of electronic surveillance are conducted in secret while the execution of a search war-

¹ 441 U.S. 238, 249.

² *Id.* at 258-259.

³ *Id.* at n. 22.

rant is not; and third, where physical entry into private premises is necessary to install a surveillance device, not only is the privacy of the occupant's communications intruded upon, but the privacy of his physical surroundings as well.

Despite the particularly intrusive character of surreptitious entries, they are nonetheless at times necessary if we are to obtain crucial evidence of the commission of those serious felonies for which Congress has approved the use of electronic surveillance by Federal law enforcement.⁴ Surreptitious entry is employed by law enforcement officers when it is necessary for them to place a surveillance device on the premises on which the communications to be intercepted take place. For the most part, interception of wire communications can be accomplished by tapping exterior lines. Therefore, surreptitious entry generally is not required for the interception of wire communications. On the other hand, the interception of oral communications usually necessitates the placement of a concealed microphone on the premises. Surreptitious entry is then required to install, maintain, and remove these microphones. In these cases, the executing officers must proceed with a surreptitious entry both to protect the secrecy of the interception and to assure their own safety. Such entry may be accomplished by a non-forceful entry onto the premises when the occupants are not present, by a physical break-in, or by means of a ruse or subterfuge.

Under section one of this bill, the term "surreptitious entry" would be defined to include "both covert entry and entry effected by means of a ruse or subterfuge". While the dissenting Justices in *Dalia* made a distinction between entry by ruse and entry by covert means of the sort which took place in *Dalia*, the majority of the Court failed to find merit in this distinction and was of the opinion that the two modes of entry, although not requiring specific judicial approval, were equally intrusive. Although in the case of an entry by ruse the occupants will be aware of the fact that some entry has been made, they will be unaware of its purpose, which is the very aspect of the entry which will prove most intrusive. Thus I believe that the procedures of the bill should apply equally to entries by ruse and those which are covert physical entries.

Title III presently requires, in addition to the probable cause showing mandated by the Fourth Amendment, that a showing be made by the applicant and that a determination be made by the issuing judge that the interception of communications is reasonably necessary. These proposed amendments to title III would simply require that a like showing be made with respect to the use of surreptitious entry to effect the interception. While the proposed procedures provide important safeguards against improper use of secret entries, they are sufficiently flexible that they may be met in appropriate circumstances. Indeed, as the section-by-section analysis which accompanied the bill pointed out, in those cases in which the interception of oral, as opposed to wire, communications is approved, surreptitious entry to install a microphone on the premises will ordinarily be "required" to effect the interception and thus no extraordinary showing of necessity is mandated.

Nonetheless, these amendments will ensure that the issuing judge is aware that such a method is contemplated. Inasmuch as the interception of oral communications is relatively rare—only 13 microphone intercepts and 13 combination microphone/wire intercepts were installed in 1978⁵—it may not be correct to assume that issuing magistrates will understand that surreptitious entry is generally required to effect such interceptions.

Needed flexibility is also retained in section 4(g) of the bill which requires that written notice be given to the issuing judge of the time and method of the initial entry and of any subsequent entries. In recognition of the fact that officers on the scene may encounter unforeseen circumstances which may require a change in time or method of entry or additional entries to adjust or repair equipment, when prior written notice is not possible, such notice may be given within forty-eight hours.

It also should be emphasized that our understanding is that the notice of the method of entry need not include a detailed description of the tools or techniques used to accomplish the entry but that a generic description of the mode of entry is sufficient under the proposed amendment, although the issuing judge may, of course, require more information if he deems it necessary. Such clarifying

⁴ Those federal felonies evidence of which may be obtained through the interception of private communications are enumerated in 18 U.S.C. 2516(1).

⁵ See the statistical tables supplied by the Administrative Office of United States Courts which appear after the section-by-section analysis of the bill. 126 Cong. Rec. 11882 (daily edition, Sept. 5, 1979.)

language should be included in the bill's legislative history. We are not concerned that the issuing judge would be apprised of detailed information about our investigative techniques, but rather that if such information is required to be included routinely in the written application, then by virtue of the notice and disclosure provisions of the statute detailed information concerning our investigative techniques and technology might become widely known and thus rendered ineffective. In addition, if entry were accomplished by means of a cooperating person such as a landlord, revealing his identity could prove dangerous. This is a subsidiary issue, but one which understandably has been of great concern to our investigative agencies.

Since, as noted above, surreptitious entry is generally required only when oral communications are to be intercepted and authorizations for interception of oral communications are relatively infrequent, the incidence of surreptitious entries in surveillance operations should be low. Nonetheless, surreptitious entry constitutes a serious physical intrusion into the privacy of individuals when it does occur and as such should be subject to the procedural safeguards provided by these proposed amendments to title III which would establish a framework for informed judicial consideration of the use of surreptitious entry in this context.

EMERGENCY LIFE-IN-DANGER INTERCEPTIONS

The second important improvement which would be worked by S. 1717 is the clarification of authorization for emergency interceptions without prior judicial approval in life endangering situations. Title III purports to prohibit, "[e]xcept as otherwise provided," willful interceptions of wire and oral communications. (18 U.S.C. 2511.) Inasmuch as electronic surveillance of private conversations constitutes a search within the meaning of the Fourth Amendment (*Katz v. United States*, 389 U.S. 347 (1967)), the general rule under title III is that non-consensual interceptions are prohibited unless conducted by law enforcement officers pursuant to court orders. Nevertheless, in emergency situations the statute permits interceptions without prior judicial authorization if there are (1) conspiratorial activities threatening the national security or characteristic of organized crime,⁶ (2) grounds upon which a court order under Title III could be obtained if time permitted, and (3) an application for an order approving the interception is made within forty-eight hours. (18 U.S.C. 2518(7).) Conspicuously absent from title III is any specific provision for warrantless emergency interceptions in life endangering situations.

Section five of S. 1717 would make clear that the United States would have the authority to engage in emergency interceptions where human life is imperiled under the following circumstances. First, an emergency situation which involves an immediate danger of death or serious physical injury must exist. Second, other grounds necessary for obtaining a federal electronic surveillance order must also exist. This, in part, means that the offense involved must be one which is listed in section 2516 of title 18 and that the probable cause requirements set forth in title III must be met. Third, within forty-eight hours after the emergency interception commences, an application for an order approving the interception must be made to a federal judge.

In light of the exigency of those situations in which human life is threatened, there seems to be no reason why title III should omit a specific provision for emergency authorization in these instances. While we believe that in those relatively infrequent occasions in which emergency interceptions in life endangering situations have been authorized by the Department, there has been a legal basis for such action, the statute is not as clear as it should be that life endangering situations, as a discrete category, are covered. Certainly, it should *not* be necessary to have to strain the present language to act in the interest of saving human life, by making a determination that the situation involves, e.g. "conspiratorial activities characteristic of organized crime". Title III, which in all other respects fully addresses in a straightforward manner those issues which may arise involving electronic surveillance, should speak clearly to authorize the use of emergency surveillance power in this most compelling situation.

Situations have arisen and may arise in which terrorists or felons, while holding hostages, use an available telephone to arrange with associates a strategy to force action on their demands or a plan of escape. Similarly, there may be situations in which plans for an imminent murder are learned, but the location or identity of the victim is not known or law enforcement authorities are other-

⁶ It is anticipated that many interceptions concerning national security matters would be governed now by the Foreign Surveillance Intelligence Act of 1978, Public Law No. 95-511, 92 Stat. 1785 (1978).

wise unable to take measures to assure his safety. In such situations, the interception of communications may be necessary to protect the lives of the hostages or victims, yet time for obtaining a court order may not be available.

The stringent procedural requirements for obtaining a court order under title III, which I believe are entirely appropriate, are nonetheless inevitably quite time consuming. Therefore, delays attendant in obtaining prior court authorization may in life endangering situations effectively preclude the timely interception of communications that could prove useful in preventing loss of life. Indeed the time normally required for obtaining written court authorization may be further lengthened in an emergency situation if the authorization must be sought at a time of day when a judge is not generally available or when the very officers who would be called upon to prepare the necessary written affidavits are in the midst of negotiating with hostage takers or locating victims.

The proposed emergency life-in-danger provision is rooted in sound constitutional doctrine. The Fourth Amendment permits a warrantless search and seizure where exigent circumstances preclude postponing a search until judicial approval can be obtained. *Warden v. Hayden*, 387 U.S. 294, 298-299 (1967); see also *United States v. Dunavan*, 485 F.2d 201 (6th Cir. 1973) and cases cited therein. This bill would simply make clear the application of this principle in the context of electronic surveillance, but only in the limited circumstance in which human life is imminently endangered. Indeed, it is plain that the justification for the narrow emergency authorization proposed here—protection of human life—is at least as compelling as the present statutory bases on which emergency interception authority may be invoked.

I would like to make it clear that this proposed life-in-danger amendment would not provide a means of circumventing the safeguards presently provided by title III. First, the approval of the Attorney General or an Assistant Attorney General must be obtained before an emergency interception may be commenced. Second, in order to obtain such approval, it must be demonstrated not only that there exists a genuine life endangering situation, but also that there is a sufficient factual basis that a title III judicial order could be obtained if time permitted. The Department views interceptions under 18 U.S.C. § 2518(7) as permissible only in the gravest emergency situations, and as a result relatively few such authorizations have been granted, nearly all of which have involved life-threatening circumstances. Third, an application for a court order approving the emergency interception must be made within forty-eight hours. Fourth, where a warrantless interception is improperly employed, severe sanctions are triggered, for title III provides for the imposition of civil and criminal sanctions and for the suppression of evidence which is illegally obtained.

In short, we believe that in light of the exigency of those situations in which human life is endangered and the existence of substantial safeguards against abuse of this proposed amendment—an amendment which we reiterate is based on sound constitutional precedent—the focus of title III's emergency electronic surveillance provision should be amended as provided in this bill to clearly include the concept of imminent danger to human life or safety. The National Commission for the Review of State and Federal Laws Relating to Wiretapping and Electronic Surveillance agreed that such an amendment was needed.⁷

Thank you for this opportunity to set forth the Department's views on S. 1717. I would be pleased to try to answer any questions or to provide the Subcommittee with any additional information it would find helpful in its consideration of this legislation.

Senator LEAHY. Mr. Colwell.

STATEMENT OF LEE COLWELL, EXECUTIVE ASSISTANT DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Mr. COLWELL. Thank you, Senator.

Senators and members of the Judiciary Committee staff, I appreciate the opportunity to discuss with you, on behalf of Director Webster and the FBI, the proposed amendments to Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

⁷ Electronic Surveillance. Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, 16, 181 (1976).

Representatives of the FBI and members of your staff have had a long series of meetings and discussions regarding the proposed changes. As a general statement, I would like to say that the FBI, along with your committee and the Department of Justice, regards electronic surveillance to be of continuing paramount concern in that such activities are among the most sensitive means of obtaining evidence of a crime. As required in the statute and reinforced in our own internal policy, such techniques demand the closest of scrutiny. When the obtaining of oral conversations pursuant to the statutes also includes the need for surreptitious entry, additional concerns arise because most installations of microphones involve breaking and entering into a private location in secrecy. Senator Kennedy has taken appropriate notice of the sensitivity of these techniques in his statement on the introduction of the proposed amendment.

The FBI has an important additional concern in carrying out surreptitious entries in that we consider such activities among the most dangerous for our agents. Our agents are well aware of the danger in making a covert entry, its intrusiveness, and the rigid requirements of the law.

The amendments dealing with surreptitious entries would require: (1) That the applicant for a Title III intercept order state in his application whether a surreptitious entry will be required to effect the interception and, if so, why other means of accomplishing the same objectives are not feasible; (2) that the issuing judge determine that such entry is reasonably required to effect the interception; and (3) that the intercept order itself specifically state whether a surreptitious entry is authorized to execute the intercept order; and (4) that the Government attorney in charge of the investigation notify the issuing court of the time and method of the proposed entry.

I will address these changes as they are listed.

Change No. 1, in section 2 of the bill, requires that an applicant for an intercept order state whether a surreptitious entry will be made and why other means of accomplishing the objectives are not feasible. Certainly, if means other than forced covert entry are available to the FBI, we would likely choose such an alternative procedure in order to reduce the element of danger to our agents.

As a practical matter, it is rare that a microphone can be installed by means other than a forced covert entry. This Congress and the courts have consistently recognized this point in reviewing covert entries.

The second proposed requirement is that the issuing judge make a determination whether a surreptitious entry is reasonably required to effect an interpretation. It is currently a requirement of both the FBI and the Department of Justice that the question of surreptitious entry is presented to the issuing judge for his consideration.

The third provision of the proposed amendment would mandate that the intercept order specifically state whether a surreptitious entry is authorized. As we all recognize, the rationale of the court in *Dalia* was, in part, based upon a finding that authorization for a surreptitious entry is implicit when a judge authorizes intercept of oral communications. This proposed amendment codifies that finding and the FBI fully supports it. The FBI completely supports the first three proposed amendment provisions.

The fourth recommendation is that the Government attorney in charge of the investigation notify the issuing court of the time and method of proposed entry. As you are probably aware, and as reflected in the reports prepared by the Administrative Office of the U.S. Courts, there have been very few Title II microphones installed that were not installed by the FBI. During the first 10 years that the statute has been in effect there were less than 182 microphone court orders for the entire Federal Government. As I said before, the FBI has made the vast majority of these installations. Our experience in case after case has shown that due to a number of unforeseeable variables, it is often impossible to predict the time or method of entry. In one case our agents were unable to effect an installation for 8 consecutive days and nights before being successful on the 9th day. Sometimes we have been unable to effect the installation at all. These variables include uncontrollable circumstances wherein "street traffic" is such that a decision is made to delay an attempted entry. Sometimes we have found it too risky to make an approach to the target location for the purpose of surveying the location until the actual entry is attempted, therefore precluding any preknowledge of the method of entry. Often the method of entry is changed when our agents reach the outer perimeter of the target location. There are only a limited number of methods available to us for effecting a covert entry, certainly we could list a number of them today; however, a technical description of those methods would only educate the criminals if they had access to them. Time and again, members of organized crime have attempted to thwart our capability for effecting covert entry. If we were required to completely describe a proposed method of covert entry to an issuing judge, such a method might very well be discoverable by the defense and quickly would become a matter of public record; thus, effectively eliminating one of those few tools available for a successful covert entry.

I quote from the section-by-section analysis of this bill, "The statement of the proposed method of entry need only indicate whether contemplated entry is to be gained by a ruse, a subterfuge, by a physical break in, or some other method, and need not detail every aspect of the mode of entry." This seems unclear and a bit contradictory. If parts of this statement were incorporated into the statute and limited to words such as "The proposed method of entry need only indicate whether contemplated entry is to be gained by a ruse, a subterfuge, or by a physical break in," we would find such a provision to be totally workable and acceptable and would not jeopardize the future use of this invaluable investigative technique. Additionally, we would be prepared to orally brief the issuing judge on additional details of the entry if the judge desired, as Mr. Heymann mentioned a few moments ago. As we have found, and I hope you understand, surreptitious entries are difficult and unpredictable. The installation of listening devices has sometimes been the only method wherein we can successfully obtain evidence against the highest levels of organized crime activity or other criminal activity in this country.

Our methods of effecting covert entry in criminal investigations are the same as those used in our foreign counterintelligence investigations; therefore, the proposed amendment concerning time and method of entry acquires additional concern which is obvious. It is

our strong belief that public revelation of our methods of effecting covert entry will effectively eliminate microphone coverage in cases involving the highest levels of organized crime, white collar crime, and foreign counterintelligence, especially any organization or entity or individual that has the funds or the money to circumvent any efforts that we might make.

Of equal significance to the FBI is the proposed change in section 2518(7) which would add another emergency situation in which a wire or oral communication could be intercepted prior to judicial approval. The interception could be authorized by the U.S. Attorney General where there is " * * * immediate danger of death or serious physical injury to any person * * * ."

Currently, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, only permits authorization of emergency interception of wire or oral communication with respect to "conspiratorial activities threatening the national security," and "conspiratorial activities characteristic of organized crime." Crimes involving possible death or serious injury unless covered by the above-described exceptions do not come under the statute. It is the view of the FBI that there is a critical need for this legislative change to authorize Title III surveillance to assist in the prevention of death or serious injury.

The FBI has been and continues to be involved in investigations where life-threatening situations arise. In most instances we are talking in terms of a hostage situation, a kidnaping, an extortion, or the planning of an execution.

The requirements of a nonemergency Title III intercept are such that from the beginning stages of an affidavit preparation until it is signed by the issuing judge takes a minimum of 2 days working around the clock. The average amount of time required for achieving routine title III intercepts is approximately 2 weeks; therefore, foreclosing our ability to acquire immediate evidence in life-threatening situations.

In addition to obtaining the evidence of a planned crime or a crime in progress, the proposed provision would allow us to react immediately in a way to better assure the safety of the victim. For example, we could identify the kidnaper, the intentions of the kidnaper, the location of the victim, or better negotiate the safe release of hostages. The FBI could more effectively anticipate the subject's moves and be in a better position to resolve the crisis without loss of life. Such information would be acquired through a tap on a phone, a microphone secured in a house or in a getaway car.

Currently, when a life-threatening situation exists and probable cause information is forthcoming, we have attempted to interpret the "conspiratorial activities of organized crime" in the broadest possible way in order to obtain the means for possibly saving a life. Some situations will not fit such a broad interpretation and it is imperative that Title III be amended in order to cover heinous felonies endangering human life.

We have included for your information a listing of some cases which involved life-threatening situations wherein the Title III surveillance may have assisted in saving a life. It is my hope that these cases will indicate how valuable a technique the emergency authority could be in life-threatening situations.

If I may, we would like to submit those for the record.

Senator LEAHY. Yes.

Mr. COLWELL. That is my statement. I would be happy to answer any questions that you might have.

[The prepared statement of Mr. Colwell follows:]

PREPARED STATEMENT OF LEE COLWELL

Senators and members of the Judiciary Committee staff, I appreciate this opportunity to discuss with you, on behalf of Director Webster and the Federal Bureau of Investigation (FBI), the proposed amendments to title III of the Omnibus Crime Control and Safe Streets Act of 1968. Representatives of the FBI and members of your staff have had a long series of meetings and discussions regarding the proposed changes. As a general statement, I would like to say that the FBI, along with your Committee and the Department of Justice, regards electronic surveillance to be of continuing paramount concern in that such activities are among the most sensitive means of obtaining evidence of a crime. As required in the statute and reinforced in our own internal policy, such techniques demand the closest of scrutiny. When the obtaining of oral conversations pursuant to the statutes also includes the need for surreptitious entry, additional concerns arise because most installations of microphones involve breaking and entering into a private location in secrecy. Senator Kennedy has taken appropriate notice of the sensitivity of these techniques in his statement on the introduction of the proposed amendment. The FBI has an important additional concern in carrying out surreptitious entries in that we consider such activities among the most dangerous for our Agents. Our Agents are well aware of the danger in making a covert entry, its intrusiveness, and the rigid requirements of the law.

The amendments dealing with surreptitious entries would require: (1) that the applicant for a title III intercept order state in his application whether a surreptitious entry will be required to effect the interception and, if so, why other means of accomplishing the same objectives are not feasible; (2) that the issuing judge determine that such entry is reasonably required to effect the interception; (3) that the intercept order itself specifically state whether a surreptitious entry is authorized to execute the intercept order; and (4) that the government attorney in charge of the investigation notify the issuing court of the time and method of the proposed entry.

I will address these changes as they are listed.

Change number one (in section two of the bill), requires that an applicant for an intercept order state whether a surreptitious entry will be made and why other means of accomplishing the objectives are not feasible. Certainly, if means other than forced covert entry are available to the FBI, we would likely choose such an alternative procedure in order to reduce the element of danger to our Agents.

As a practical matter, it is rare that a microphone can be installed by means other than a forced covert entry. This Congress and the courts have consistently recognized this point in reviewing covert entries.

The second proposed requirement is that the issuing judge make a determination whether a surreptitious entry is reasonably required to effect an interception. It is currently a requirement of both the FBI and the Department of Justice that the question of surreptitious entry is presented to the issuing judge for his consideration.

The third provision of the proposed amendment would mandate that the intercept order specifically state whether a surreptitious entry is authorized. As we all recognize, the rationale of the court in *Dalia* was, in part, based upon a finding that authorization for a surreptitious entry is implicit when a judge authorizes intercept of oral communications. This proposed amendment codifies that finding and the FBI fully supports it. The FBI completely supports the first three proposed amendment provisions.

The fourth recommendation is that the government attorney in charge of the investigation notify the issuing court of the time and method of the proposed entry. As you are probably aware, and as reflected in the reports prepared by the Administrative Office of the United States Courts, there have been very few title III microphones installed that were not installed by the FBI. During the first ten years that the statute has been in effect there were less than 182 microphone court orders for the entire Federal government. As I said before, the FBI has made the vast majority of these installations. Our experience in case after

case has shown that due to a number of unforeseeable variables, it is often impossible to predict the time or method of entry. In one case our Agents were unable to effect an installation for eight consecutive days and nights before being successful on the ninth day. Sometimes we have been unable to effect the installation at all. These variables include uncontrollable circumstances wherein "street traffic" is such that a decision is made to delay an attempted entry. Sometimes we have found it too risky to make an approach to the target location for the purpose of surveying the location until the actual entry is attempted, therefore precluding any preknowledge of the method of entry. Often the method of entry is changed when our Agents reach the outer perimeter of the target location. There are only a limited number of methods available to us for effecting a covert entry, certainly we could list a number of them today; however, a technical description of those methods would only educate the criminals if they had access to them. Time and again, members or organized crime have attempted to thwart our capability for effecting covert entry. If we were required to completely describe a proposed method of covert entry to an issuing judge, such a method might very well be discoverable by the defense and quickly would become a matter of public record; thus, effectively eliminating one of those few tools available for a successful covert entry.

I quote from the section-by-section analysis of this bill, "The statement of the proposed method of entry need only indicate whether contemplated entry is to be gained by a ruse, a subterfuge, by a physical break in, or some other method, and need not detail every aspect of the mode of entry." This seems unclear and a bit contradictory. If parts of this statement were incorporated into the statute and limited to words such as "The proposed method of entry need only indicate whether contemplated entry is to be gained by a ruse, a subterfuge, or by a physical break in," we would find such a provision to be totally workable and acceptable and would not jeopardize the future use of this invaluable investigative technique. Additionally, we would be prepared to orally brief the issuing judge on additional details of the entry if the judge desired.

As we have found, and I hope you understand, surreptitious entries are difficult and unpredictable. The installation of listening devices has sometimes been the only method wherein we can successfully obtain evidence against the highest levels of organized crime activity or other criminal activity in this country.

Our methods of effecting covert entry in criminal investigations are the same as used in our Foreign Counterintelligence investigations; therefore, the proposed amendment concerning time and method of entry acquires additional concern which is obvious. It is our strong belief that public revelation of our methods of effecting covert entry will effectively eliminate microphone coverage in cases involving the highest levels of organized crime, white collar crime, and foreign counterintelligence.

Of equal significance to the FBI is the proposed change in section 2518(7) which would add another emergency situation in which a wire or oral communication could be intercepted prior to judicial approval. The interception could be authorized by the United States Attorney General when there is "... immediate danger of death or serious physical injury to any person ..."

Currently, title III of the Omnibus Crime Control and Safe Streets Act of 1968, only permits authorization of emergency interception of wire or oral communication with respect to "conspiratorial activities threatening the national security," and "conspiratorial activities characteristic of organized crime." Crimes involving possible death or serious injury unless covered by the above-described exceptions do not come under the statute. It is the view of the FBI that there is a critical need for this legislative change to authorize title III surveillance to assist in the prevention of death or serious injury.

The FBI has been and continues to be involved in investigations where life threatening situations arise. In most instances we are talking in terms of a hostage situation, a kidnapping, an extortion, or the planning of an execution.

The requirements of a nonemergency title III intercept are such that from the beginning stages of an affidavit preparation until it is signed by the issuing judge takes a minimum of two days working around the clock. The average amount of time required for achieving routine title III intercepts is approximately two weeks; therefore, foreclosing our ability to acquire immediate evidence in life threatening situations.

In addition to obtaining the evidence of a planned crime or a crime in progress, the proposed provision would allow us to react immediately in a way to better assure the safety of the victim. For example, we could identify the kid-

naper, the intentions of the kidnaper, the location of the victim, or better negotiate the safe release of hostages. The FBI could more effectively anticipate the subject's moves and be in a better position to resolve the crisis without loss of life. Such information would be acquired through a tap on a phone, a microphone secured in a house or in a getaway car.

Currently, when a life-threatening situation exists and probable cause information is forthcoming, we have attempted to interpret the "conspiratorial activities of organized crime" in the broadest possible way in order to obtain the means for possibly saving a life. Some situations will not fit such a broad interpretation and it is imperative that title III be amended in order to cover heinous felonies endangering human life.

I have included for your information a listing of some cases which involved life threatening situations wherein the title III surveillance may have assisted in saving a life. It is my hope that these cases will indicate how valuable a technique the emergency authority could be in life threatening situations.

CASE STUDIES OF FBI INVESTIGATIONS DEMONSTRATING A NEED FOR EMERGENCY AUTHORIZATION FOR WIRE OR ORAL COMMUNICATION INTERCEPTION IN LIFE THREATENING SITUATIONS

MARK ANTHONY HAYNES; DONNA CRAIG—VICTIM;
HOBBS ACT—COMMERCIAL INSTITUTION

On October 4, 1979, a then unknown subject, later identified as Mark Anthony Haynes, residing in Atlanta, Georgia, entered the Executive Office of Edward W. Rabin, Jr., Regional Vice-President and General Manager, Hyatt-Regency Hotel, 265 Peachtree Street, N.E., in downtown Atlanta, Georgia. The subject immediately demanded twenty thousand dollars after producing a handgun. Mr. Rabin agreed to obtain the twenty thousand dollars, and left the Executive Office, leaving Ms. Donna Craig, a Hyatt-Regency Executive Secretary as hostage with Haynes in the Executive Office. Mr. Rabin notified the Atlanta Bureau of Police Services, and the Atlanta, FBI.

Telephone negotiations were established between the hostage negotiators and the subject, such negotiations continued off and on for the next twenty hours. During that period, a brief glimpse of the subject at the window of the office revealed that he was armed with a handgun. During other periods when there was no telephone contact with the subject, the status and welfare of the hostage were unknown.

On October 5, 1979, as a result of the hostage negotiations, the subject was given twenty thousand dollars, whereupon he released the hostage. He proceeded to a taxi parked at the entrance to the Hyatt-Regency, which was to be the getaway vehicle pursuant to the negotiations. He entered the vehicle, and when it would not start, he gave up without further incident.

Reconnaissance efforts undertaken during the investigation indicated that a microphone could have been placed in the ceiling directly above where the hostage and the subject were located. If such a procedure had been available, it would have been extremely valuable in monitoring the conversation between the subject and hostage, and more accurately assessing the danger to the hostage.

PABLO MARCANO GARCIA; NYDIA ESTHER CUEVAS RIVERIA; PUERTO RICAN NATIONALIST
TAKEOVER OF CHILEAN CONSULATE, JULY 3, 1978

On July 3, 1978, the Chilean Consulate to Puerto Rico was taken over by force by Marcano and Cuevas. They were holding an unknown number of hostages, including Ramon Gonzalez Ruiz, the Honorary Consul of Chile.

Negotiations for the release of the hostages were immediately instituted. During the negotiations, the abductors continuously threatened the lives of the hostages should their demands not be met. It was determined that emergency authority for wire or oral communications interception could not be granted under title III in this case.

That day, the Attorney General of the United States authorized application to a Federal Judge of competent jurisdiction for an order authorizing the interception for a period of ten days of wire and oral communications in connection with the investigation of the possible violations of title 18, United States Code, involving murder, kidnaping, or extortion.

At approximately 10:50 a.m., on July 4, 1978, the abductors surrendered to the Federal Bureau of Investigation, having been satisfied through the negotiating process that their demands were met to the degree required. An attempt was made to secure title III authority under normal procedures; however, this surrender occurred before authority could be granted.

The availability of wire and oral intercepts from the very inception of the hostage situation would have aided in the negotiation process immeasurably by furnishing information concerning their arms, and details about their plans so that the FBI could better anticipate their moves.

UNKNOWN SUBJECT; CARY SAYEGH—VICTIM; KIDNAPING

On October 25, 1978, Cary Sayegh, six years old, disappeared from the Albert Einstein School playground in Las Vegas, Nevada between 12:00 noon and 12:30 p.m. At approximately 3:30 p.m., on the same date, the family received a telephone call from the alleged abductor who stated he wanted \$500,000 ransom, and would call back midday, Friday, October 27, 1978, with further instructions. As of this day, the family has received no additional telephone calls, Cary Sayegh is still missing, and the case unsolved.

Early in the investigation, a suspect was developed and interviewed several times. The suspect advised that he was in no way connected with the kidnaping case; however, he did state that the kidnapers had contacted him and asked that he be the intermediary between the kidnapers and the Sayegh family. As the result of this alleged position, this suspect stated that he would be receiving telephone calls at certain pay telephone booths from the kidnapers involving further negotiations on the delivery of the child and the ransom money to be paid. He provided little other assistance. Surveillance of this suspect conducted by the FBI reflected that he apparently received telephone calls from several pay telephones. According to the suspect, one of these telephone calls provided information as to the whereabouts of one of the boy's shoes. The boy's shoe was found by the family in the location where the suspect told them it would be found.

It was during the time when the suspect was allegedly making and receiving telephone calls to the kidnapers that emergency authorization for wire communication interception would have been most valuable in determining if such kidnapers existed, and if so, their identities. In addition the technique could have possibly contributed towards location of the victim since the victim's whereabouts may have been discussed during the calls.

LARRY DONALD SMITH; CAROLYN MARYANN BEALER—VICTIM; HOBBS ACT—
COMMERCIAL INSTITUTION

On August 23, 1979, Mr. Lawrence Paul Fox, a partner in the Active Construction Clean-up Company, Los Angeles, California, received a telephone call from his sister, Carolyn Maryann Bealer. She advised her brother that she had just been kidnaped. Her abduction was subsequently confirmed at that time, by an unidentified male telephone caller, who later demanded \$100,000 cash ransom for her release. By the use of a consensually monitored telephone conversation and telephone call tracing, Larry Donald Smith was developed as a suspect during the late evening of August 25, 1979. On August 26, 1979, Larry Smith voluntarily submitted to an interview with the FBI, after having contacted the Newport Beach Police. He admitted making all the telephone calls in this matter and stated that he had been coerced and forced to participate in the kidnap ransom plan by two unknown males. Smith has since been prosecuted, convicted, and sentenced in this matter. Carolyn Bealer has not been located as of this date, and is feared to have been murdered.

Emergency authorization for wire communication interception on the residential telephone of Larry Smith from the time he was developed as a suspect could have greatly contributed to the safety of the victim, by leading possibly to the identities of the unknown males and location of the victim.

HANAFI MUSLIM SECT (HMS), WASHINGTON, D.C., DOMESTIC SECURITY
INFORMATION CONCERNING

On March 9, 1977, 12 armed men identified as members of the HMS forced their way into the B'nai B'rith International Headquarters, the Washington, D.C., District Government Building, and the Islamic Center in Washington, D.C.

(WDC). During the initial stages of these hostage situations a number of individuals were injured, one fatally, and more than 100 hostages were taken and held. On the morning of March 11, 1977, these individuals surrendered to Metropolitan Police Department (MPD) and at that time, were fully identified. Ernest Timothy McGhee, also known as Hamaas Abdul Khaalis, was identified as the leader of this sect.

The U.S. Attorney for the District of Columbia authorized emergency interception of telephone communications in the B'nai B'rith and District Buildings under title 23, section 23-548(a) of the D.C. Code which parallels title 17, section 2518, of the U.S. Code. Invaluable information concerning arms possessed by the subjects, their identities, the conditions of the hostages and the ultimate intent of the subjects was obtained through these wiretaps. There was delay in the obtaining of this emergency authorization due to the unclear nature of the emergency provisions.

The following table sets forth the number of court orders involving telephone and microphone surveillances conducted by the FBI since the enactment of the Omnibus Crime Control and Safe Streets Act of 1968:

	Microphone orders	Telephone orders	Orders con- taining both	Total
1968.....	0	0	0	0
1969.....	1	22	2	25
1970.....	3	138	5	146
1971.....	3	251	5	259
1972.....	5	131	12	148
1973.....	10	76	12	98
1974.....	7	71	8	86
1975.....	11	62	8	81
1976.....	10	81	15	106
1977.....	5	41	4	50
1978.....	13	38	13	64
1979.....	18	40	20	78
Total.....	86	951	104	1,141

Senator LEAHY. Thank you. I appreciate the examples you have given. I think they will be helpful to us.

I will question you briefly. Either one of you, please feel free to answer this. You have just made some allusion, Mr. Colwell, to the number of microphone eavesdrops, as I understand, from 1968 through 1978, a 10-year period. There were some 1,200 Federal taps, but you said 182 microphone eavesdrops or bugs were employed. Why is the bug used so infrequently? Is it that they are not extremely valuable or is it more difficult to get installed?

Mr. COLWELL. Well, many times the telephone—information obtained through the telephone intercept is valuable information, and if that proved to be the case, and we are obtaining evidence, there is no need to take the additional step of installing a microphone. You might jeopardize the information you are obtaining on the telephone.

It is more difficult and it requires a lot more manpower to install the microphone or the bug, and effect a surreptitious entry.

Senator LEAHY. But are wiretaps all that effective?

Mr. COLWELL. Yes.

Senator LEAHY. People who are involved, for example, in organized crime just proceed on the assumption that their phones are bugged, or do they become complacent after a while?

Mr. COLWELL. I think they go on the assumption that their phones are bugged, but it is not infrequent that you hear someone in an approved wiretap talking about this phone is probably bugged, and then they proceed then to discuss details of conspiracy or the results of a particular crime.

Mr. HEYMANN. I agree with that, Senator Leahy. I would like to add on the question of bugs versus wiretaps that I regard a microphone in a room as a somewhat more serious intrusion than a wiretap. And since I have to approve all these, I am a little tougher. This doesn't account, obviously, for the figures for the last 10 years, and it doesn't account for the type of disparities we are seeing, but I think it is appropriate to be a little bit tougher on microphones in rooms than on wiretaps, although we are tough on both of them.

Senator LEAHY. When you compare these figures of 400 versus 180, is that roughly the kind of breakdown that you are currently showing?

Mr. HEYMANN. I have figures by years here. Maybe Lee does, too; 1976 had 134 total wire and microphone interceptions; 1977 had 77 total; 1978 went up to 90. I am sure 1979 will go up some. You are still talking, though, in the neighborhood of between 100 and 200 orders for electronic surveillance in the entire country in a year. It seems to me to be a small number.

Senator LEAHY. These are Federal agencies, and, of course, on top of that is State agencies?

Mr. HEYMANN. That is correct. As for the State agencies—I forget what the numbers are. I will take a look.

Do you know, Lee?

Senator LEAHY. Not all States are involved?

Mr. HEYMANN. No. But you are quite right, including State agencies would multiply that figure several times. I think we have those figures, but I do not have them with me.

Senator LEAHY. I know in my own State——

Mr. COLWELL. Senator, we will be glad to submit the figures for the State agencies if you would like.

Senator LEAHY. I would. That would be entered into the record.

Mr. COLWELL. I would like to go back to your comment about the use or utilization of the microphones. The value of them would occur if you had a large room such as this and the telephone is located over here in this corner, and the working relationship of that particular individual with others occurs on the other side of the room, and he is not prone to use the telephone, then that would be an example where the microphone would be essential.

Also telephones are not located in all offices or in each room of a residence.

So there are circumstances where there is no substitute for the microphone.

Senator LEAHY. Would such a thing as a spike mike or a parabolic mike require covert entry of the nature that would be included under the provisions of this bill?

Mr. HEYMANN. It is my interpretation of the bill that it would generally require specific approval under the category of surreptitious entry or of a spike mike or a parabolic mike. It would, of course, still be subject to the normal Title III oral interception provisions. I believe that is right.

Mr. COLWELL. As a general statement, I would say that we would—our position would be that the installation of a spike mike would always involve some type of entry if you get in proximity or some type of intrusion. That might be granted by someone in an adjoining apartment, but it would still involve intrusion nature of the equipment.

Senator LEAHY. Mr. Colwell, let me propose a hypothetical: Suppose an FBI agent in Vermont wanted to either wiretap or bug somebody in Vermont. Let us assume it is involved in organized crime of some sort. Unless they changed the laws since I was a prosecutor, there is no Vermont law that prohibits wiretapping or bugging.

What is the kind of procedure which you would follow? After all, this is not an emergency, this is not a hostage situation. Let us assume that there is going to be a meeting of organized crime figures or something of that nature in Vermont. Maybe I should have used a different example. The chamber of commerce will be after me, but what would you do? What steps would he have to follow, assuming that he has made a determination as an investigator that this would aid his investigation? What would he do next?

Mr. COLWELL. Well, there are a number of criteria that must be met by law, and assuming that that exists, the agent would, first of all, discuss it with his supervisor, the need for it. They would review whether or not all the other reasonable leads had been covered, and that there was reasonableness in asserting that there was no other way to obtain the information that was about to develop.

Then it would be discussed with the assistant U.S. attorney, or the U.S. Attorney, a proposal or application would be submitted to FBI Headquarters for review, which would also include a review of our operational people as well as our legal counsel.

Senator LEAHY. By FBI, of course, you mean back in Washington?

Mr. COLWELL. In Washington. And that is also discussed in the early stages with the departmental attorney in Mr. Heymann's division. Then the application is prepared, reviewed, and then it is submitted eventually to a judge.

Senator LEAHY. So you don't have a loose canon spreading around out there?

Mr. COLWELL. No, sir.

Senator LEAHY. Slapping out bugs, wiretaps, and so forth?

Mr. COLWELL. An agent couldn't have even—we have control, internal controls on the equipment necessary to effect such an installation.

Senator LEAHY. In other words, that had to be checked out?

Mr. COLWELL. It has to be checked out. Only certain individuals are authorized to do that, and he has to clear each utilization with the SAC, and then we have audits of our field offices that checks those uses against the authorized applications.

Senator LEAHY. Aside from the case law and various types of exclusionary rules, does this encourage agents, rather than going through all the required procedure to go to a local sheriff who might have easy access to the country prosecutor, whatever, to get a wiretap and say, "Look, I know I am never going to get this thing through Washington or my supervisor so how about you guys going in and tapping this motel or this office and let me know what you find out?"

Mr. COLWELL. Even if that should occur, which I don't think it can occur with our administrative controls right now that have been adopted in the past 5 years, even if that should occur, he would at some point have to identify the source of that information to the U.S. attorney and to his superiors in the FBI. He could not do that without its becoming known later if the case is to be tried.

Mr. HEYMANN. Senator Leahy, it may be mere coincidence, but I don't think I have seen a case since I have been at the Justice Depart-

ment, in which we have relied in any way on evidence obtained from a State court ordered electronic surveillance.

In other words, I can't remember, as I sit here, any such case. I am sure they exist, but just to give you an idea it is not very frequent, I can't remember seeing a case where what we were doing federally in some way turned upon State-ordered electronic surveillance.

I think what you are asking is whether an FBI agent who found it difficult to get approval—and it is difficult to get an approval for electronic surveillance through the Federal system—would just turn to his State counterpart and say, "Why don't you run it through the State system?"

He could do that, but it would result in a State trial. In effect, he would simply be suggesting to his State counterpart that this would be a good State case.

My guess is it is very rare that an agent does that as a way of getting evidence for a Federal trial. I just know I haven't seen any since I have been there, and it is almost 2 years.

Senator LEAHY. I am well aware of the silver platter cases on that.

Mr. COLWELL. Senator, where this has occurred in prior instances, our internal procedure requires the same steps at the State level if we are going to participate in that information collection. The same steps that are required in the Federal process also be applied to the State application.

Senator LEAHY. Obviously, I am not going to sit here and swap war stories, but for a number of years I was the prosecutor and served as one of the vice presidents of the National District Attorney's Association, and one of my responsibilities was to go around lecturing to various prosecutors, groups around the country involved in law enforcement.

I recall discussions of wiretapping and many times I felt that there is a glamour and mystique about wiretapping and bugging. My own experience was that it was a very rare case that might turn on a wiretap or a bugging. When it does become an essential tool, and it really is an essential tool in cases involving organized crime, and hostage kidnapping. You don't find too many two-bit burglars that way and we shouldn't be trying to expand that kind of intrusion for case where it isn't essential.

The only point I am making is that I would hope that you would maintain very, very tight internal standards within the FBI, and within the Department of Justice itself. I think what you will find intrusive activity in States when they decide to have a State wiretap or bugging statute.

Now, they'll look at whatever the Federal model is, and I would hope they would look at it with the idea of restraint rather than the other way around, because as an effective necessary law enforcement tool, whether we like it or not, wiretapping and bugs will have to be used. I think that to maintain the civil liberties of our people as well as to maintain the credibility of law enforcement, these methods should be used very, very sparingly.

I would hope that to the extent you are asked for advice from State legislatures, you would emphasize over and over again tight internal controls that such intercepts should really be the exception and not the rule. Apparently these numbers speak for themselves.

I can think of instances where an unchecked head of the State agencies themselves would have problems you have had nationwide. I would hope you would be very, very careful.

Mr. COLWELL. Senator, I think we can assure you that we will continue our stringent controls and use it sparingly. I would only point out for the record that types of crimes are cyclical in that—

Senator LEAHY. Some types of crime are what?

Mr. COLWELL. Some types of crimes become a fad. Hostage taking right now is an example, and—

Senator LEAHY. Airplane hijacking.

Mr. COLWELL. Hijackings, and at any given time if you look over a 10-year period, we might see an increase in the use of this technique, but it would be tied to the criminal activity, not because we were loosening our goals.

Senator LEAHY. I see.

Mr. HEYMANN. I would like to say the same thing in a more specific way, Senator Leahy, because I think Lee is absolutely right.

My predecessor who is now Attorney General simply said that he would not approve a Title III, I have to approve all criminal electronic surveillance in a gambling-type situation. That vastly reduced the total numbers of Title III's. That policy wasn't absolute. There are rare exceptions where a gambling operation is big enough, but this policy substantially reduced the number of such interceptions and the FBI agreed. What happens to some extent is that when one category disappears, the sophisticated and talented agents in the field will look for other strong and proper cases, cases where, for example, they have a "hit" man instead of a gambler; cases that previously had not involved the use of electronic surveillance. The result of it is that figures will reflect some variance with each year.

They were up at about 134 in 1976. They dived precipitously in the year 1977 to about 77. The figure for 1978 is 90. It will all go up again in the direction, I think it is, of 100, or in the neighborhood of 150 cases out of 30,000 Federal prosecutions.

This does not reflect a change in attitude toward the seriousness of the cases. It reflects the fact that when you make the attitude clear, the system adjusts a little bit and starts finding very serious cases.

Senator LEAHY. I am far more interested in the nature of the cases than the numbers.

Mr. HEYMANN. That is what I have tried to do.

Senator LEAHY. But I think the whole point, of course, is that it is—you are going to be watched so much by a State agency, and I just emphasize and reemphasize and reemphasize the type of controls, because I think there is, many times in law enforcement agencies around the country, a kind of glamour idea of somebody going in and slapping a bugging device or a wiretap and cracking the big case and so on.

But unfortunately, sometimes that is done as an alternative to the type of hard, dull work that is necessary to crack the case without it.

I have a number of questions that I would like to submit for the record, and these—you can take these questions and make sure the staff gets them to you, and I think they would be helpful to the legislative record of this—we all know that when you get the one case that none of us have been able to anticipate, and somebody is going to come

back through the record and try to find out what the intent was, so I will submit those and then having answered those, gentlemen, if you have further statements that you want to submit, we will keep the record open for that purpose.

Mr. HEYMANN. Thank you, Senator Leahy, we will be delighted.

Senator LEAHY. Thank you for both being here.

Mr. COLWELL. Thank you, Senator.

Mr. HEYMANN. Senator Leahy?

Senator LEAHY. Yes, sir.

Mr. HEYMANN. I want to say to you that this has been undoubtedly the finest 8 a.m. hearing I have ever been to.

Senator LEAHY. I apologize for making it so late, but by 7 o'clock, my 6 o'clock schedules were already filled.

Look how it gives you a chance to get back to the office now, wide awake, ready to go and gets you off the Hill for a change. Is it the earliest you have been off the Hill?

Mr. HEYMANN. It is the earliest I have ever been up on the Hill.

Senator LEAHY. Thank you.

Mr. COLWELL. Thank you, Senator.

Senator LEAHY. Mr. Fishman.

Our next witness is Clifford S. Fishman, Associate Professor of Law at Catholic University.

Mr. Fishman, I point out first that you come here with glowing recommendations from Senator Mathias. He would have been here today, but he is in Baltimore, and sends his best and tells me to listen with great care to whatever you have to say.

Mr. FISHMAN. I appreciate that.

Senator LEAHY. I want you all to know that.

STATEMENT OF CLIFFORD S. FISHMAN, ASSOCIATE PROFESSOR OF LAW, CATHOLIC UNIVERSITY OF AMERICA

Mr. FISHMAN. Thank you very much.

I want to thank the committee, and you, Senator Leahy, for giving me the opportunity to testify concerning S. 1717. In the hope that it may be helpful, I have taken the liberty of preparing a brief memorandum of law to amplify my remarks. And that will be distributed later to the members of the committee.

Senator LEAHY. I read the memo of law, and that will be made part of the record together with your statement.

Mr. FISHMAN. For 8 years I served as an assistant district attorney in the New York County District Attorney's Office. During this period I wrote, supervised the execution of, and litigated the validity of 40 wiretaps and bugs. I would think 32 wiretaps and 8 bugs were roughly the breakdown, give or take 1 or 2.

Since joining the faculty of the Catholic University of America School of Law, I have published a treatise on the subject, so I am familiar with the general area discussed in the bill.

Overall, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 constitutes an excellent balance between the needs of law enforcement and the protection of individual privacy. Three aspects of Title III, however, are unsatisfactory.

First, the emergency surveillance provision as it now exists may preclude the use of electronic surveillance when the need is greatest, that is, when there is an immediate threat to human life or safety.

Second, the statute contains no provision regulating covert entry to install or maintain listening devices.

Third, the minimization provision, particularly as interpreted by the Supreme Court in *Scott v. United States*, affords inadequate protection to the privacy of those whose phones are tapped or whose premises are bugged.

S. 1717 corrects the first two shortcomings I mentioned. Section 5 of the bill, dealing with emergency surveillance, is based on sound public policy and sound constitutional doctrine. Protection of human life and safety is law enforcement's single most important function. This provision will enable law enforcement to fulfill that function without intruding upon legitimate privacy interests in any significant way. It merits passage.

The first four sections of S. 1717, dealing with surreptitious entry, also merit passage. The bill provides a broad, workable definition of surreptitious entry. It specifies what the application for an interception order must contain; sets forth an appropriate standard against which the issuing judge is to measure the application; it spells out what the order must contain. It does so clearly and straightforwardly in language that even a law professor can understand.

The section-by-section analysis that accompanied the bill's introduction on the floor of the Senate provides additional practical guidance to the meaning and impact of the proposal. Thus, for example, the analysis makes it clear that in bugging situations, the need for surreptitious entry may be demonstrated simply by stating that no reliable equipment is available that would permit the interception of oral communications from outside the premises. Further, the method of entry need only be stated in general terms, unless the judge specifically requests additional information. Even if one method has been chosen, the proposal gives the agents the flexibility to take advantage of a fleeting opportunity to use a safer or less conspicuous method.

There are, however, a few aspects of the bill that may merit further clarification, if further clarification is possible. I have addressed these in my memorandum. I will mention only two here.

First, the proposal does not require that those with a privacy interest in the premises ultimately be notified of how many surreptitious entries were made or when. It would be worthwhile to amend 18 U.S.C. 2518 (8) (d), the statutory inventory and notice provision, by adding a new subparagraph: "(4) if surreptitious entries were made onto premises, the number and dates of such entries."

The second aspect of the statute worth additional attention is the question of how to assess the propriety of the method of entry chosen. In *Dalia v. United States*, the Supreme Court held that the manner in which law enforcement officials execute a warrant is subject to a fourth amendment standard of reasonableness. S. 1717 does not provide any more precise standard. Perhaps it would be impossible to provide a more precise standard and unwise to try. Without a more precise standard in the statute, the courts will have to consider the question as it arises on a case-by-case basis.

Overall, then, S. 1717 fills two of the three significant shortcomings in Title III. It merits passage.

I understand that the FBI and DEA have expressed concern that if a defendant is allowed to learn the time or method of entry, this might jeopardize the safety of cooperating individuals or compromise the future effectiveness of that method. That is a very legitimate concern. I know I had a similar experience when I was a prosecutor in New York.

There was one particular narcotics organization that we were constantly trying to break and constantly failing. We later learned that one of the reasons was that this organization regularly sent observers who sat in on trials and hearings and took notes as to what techniques we were using. These observers would report back to their superiors, and their superiors would adjust their own evasion techniques accordingly. Eventually they got sloppy or we got lucky, and the organization was broken, but I think the concern is legitimate.

The other side of the coin is that a defendant has the right, must be given the right, to challenge the validity of the seizure of evidence that is being used against him. He is given notice that there was a wiretap or a bug. He certainly has a right to challenge the papers.

At some point there has to be some judicial examination of whether the method of entry in a surreptitious entry situation was reasonable.

Senator LEAHY. How do you balance it, for example, if you apply time and method laws in a court hearing? Assuming these follow certain patterns, do you use them in certain types of organized crime? If you go into an evidentiary hearing on time and method log, might that not well preclude the type of surveillance method to be used in a similar kind of organized crime?

Mr. FISHMAN. Yes; as I said, it is a substantial problem. The question would be—at some point I think a judge, whether it be the judge who issues the eavesdropping order, or the judge who subsequently conducts the suppression hearings, but at some point a judge is going to have to make a judicial decision whether the warrant was executed in a reasonable fashion. That has always been the fourth amendment test. The Supreme Court repeated that in the *Dalia* decision.

I listened to the comments of Assistant Attorney General Heymann and the representative of the FBI today, and again, they expressed a valid concern.

Still, at some point the prosecutor is going to have to explain to a judge how entry was effected and why that method was chosen, so the judge has a basis to say, "All right, under the circumstances I conclude this is a reasonable method."

If the statute would permit that explanation to the judge who issued the warrant, perhaps it could thereby preclude the defendants from learning how it was done. Still, if we prevent them from learning how entry was effected, we are obviously preventing them from litigating the reasonableness of the method chosen.

At least at some point a judicial officer has made that assessment, even if it is *ex parte* before the defendant is ever arrested.

Senator LEAHY. Then you hear the argument on the other side, that they should know everything.

Mr. FISHMAN. I think the presumption should be in favor of allowing the defendant at least general information, the time of day, and

there are only 24 hours a day. My own experience has been telling someone that we snuck in at 2:30 in the morning doesn't tell the criminal community something they haven't already figured out. It is easier for law enforcement to be covert or surreptitious at 2:30 in the morning.

Senator LEAHY. Suppose you told them it was done between 2 and 3 o'clock in the afternoon. The bug was placed in his office, and he knows he was in the office between 2 and 3, and there is only one person who came in, his trusted employee. It pretty well points out that the trusted employee is getting a double salary, the other salary being from the FBI.

Mr. FISHMAN. I think that should—

Senator LEAHY. The organized crime aspect, may make that employee a candidate for whole life insurance.

Mr. FISHMAN. I agree. I agree. We have had not precisely that experience in New York, but similar experiences. I still think the presumption should be in favor of disclosure. I think, though, that perhaps either in the legislative—probably in the legislative history might be the best place to develop this.

A procedure might be permitted whereby in a particular case if the Government has a concrete valid basis for seeking to preclude the defendant from learning how entry was effected, or how installation was effected, then an ex parte showing could be made to the judge prior to the suppression hearing, and if a judge concludes that there is, in fact, a valid basis to withhold disclosure, then the judge might conduct an ex parte hearing without the defendant or defense counsel being present to assess the reasonableness of entry.

In a sense, this borrows from some of the procedures that were adopted by the Congress in the Foreign Intelligence Surveillance Act, where the entire suppression proceeding in that statute can be ex parte. Perhaps this aspect of the Title III suppression hearing could also be ex parte where a need for such were specifically shown.

Senator LEAHY. I raise the question in an attempt to anticipate what may come up on the floor among the other 99 Members of the Senate.

I know I had my own rules as a prosecutor. I used to tell the police to hand the report to me and that whatever case they were involved in, to proceed on the assumption that they would seek prosecution afterward. At some point everything they did is going to be a matter of public record.

Mr. FISHMAN. That is a good rule of thumb.

Senator LEAHY. It may well not, but they should go on the assumption that it would and act in that light.

Having said that, however, I realize the strains that puts on everything from informants' perspective, especially when they use informants again.

I think the point I am trying to make here is that there are no easy answers. We should go on the assumption that the trends of courts are toward substantial disclosure, and democracy. I have absolutely no problem with that whatsoever.

I mention it, because the balancing is going to be done by this committee and by the Congress and by the Federal law enforcement agencies involved.

I appreciate your answers and I appreciate the brief that you have provided to the committee. It is helpful. We may have further questions as we go along, too I had hoped that we would be able to call on you and answer them.

Mr. FISHMAN. It will be my privilege.

Senator LEAHY. Thank you. I hope you are enjoying the academic after the pragmatic. In New York, was that with Mr. Hogan?

Mr. FISHMAN. Mr. Hogan and now with Mr. Morgenthau, yes, sir.

I am an alumnus of a darn good office and proud of it. It is a tremendous office. I have had occasion in the past to work with them on things. I was always impressed that it was about the best for a prosecutor to have been in one or two or three most exciting offices to be in.

Thank you very much.

[The prepared statement of Mr. Fishman follows:]

PREPARED STATEMENT OF CLIFFORD S. FISHMAN

I want to thank the Committee for giving me the opportunity to testify concerning S. 1717. In the hopes that it may be helpful, I have taken the liberty of preparing a brief memorandum of law to amplify my remarks.

For eight years I served as an assistant district attorney in the New York County District Attorney's Office. During this period I wrote, supervised the execution of, and litigated the validity of forty wiretaps and bugs. Since joining the faculty of The Catholic University of America School of Law, I have published a treatise on wiretapping and eavesdropping. Hence, I am familiar with the subject matter of this bill.

Overall, title III of the Omnibus Crime Control and Safe Streets Act of 1968 constitutes an excellent balance between the needs of law enforcement and the protection of individual privacy. Three aspects of title III, however, are unsatisfactory. First, the emergency surveillance provision as it now exists may preclude the use of electronic surveillance when the need is greatest, that is, where there is an immediate threat to human life or safety. Second, the statute contains no provision regulating covert entry to install or maintain listening devices. Third, the minimization provision, particularly as interpreted by the Supreme Court in *Scott v. United States*, affords inadequate protection to the privacy of those whose phones are tapped or whose premises are bugged.

S. 1717 corrects the first two shortcomings I mentioned. Section 5 of the bill, dealing with emergency surveillance, is based on sound public policy and sound constitutional doctrine. Protection of human life and safety is law enforcement's single most important function. This provision will enable law enforcement to fulfill that function better without intruding upon legitimate privacy interests in any significant way. It merits passage.

The first four sections of S. 1717, dealing with surreptitious entry, also merit passage. The bill provides a broad, workable definition of surreptitious entry. It specifies what the application for an interception order must contain; sets forth an appropriate standard against which the issuing judge is to measure the application; it spells out what the order must contain. It does so clearly and straightforwardly in language that even a law professor can understand.

The section-by-section analysis that accompanied the bill's introduction on the floor of the Senate provides additional practical guidance to the meaning and impact of the proposal. Thus, for example, the analysis makes it clear that in bugging situations, the need for surreptitious entry may be demonstrated simply by stating that no reliable equipment is available that would permit the interception of oral communications from outside the premises. Further, the method of entry need only be stated in general terms, unless the judge specifically requests additional information. Even if one method has been chosen, the proposal gives the agents the flexibility to take advantage of a fleeting opportunity to use a safer or less conspicuous method.

There are, however, a few aspects of the bill that may merit further clarification, if further clarification is possible. I have addressed these in my memorandum. I will mention only two here. First, the proposal does not require that those with a privacy interest in the premises ultimately be notified of how many surreptitious entries were made or when. It would be worthwhile to amend 18 U.S. § 2818(8)(d), the statutory inventory and notice provision by adding a new

subparagraph "(4) if surreptitious entries were made onto a premises, the number and dates of such entries."

The second aspect of the statute worth additional attention is the question of how to assess the propriety of how entry was effected. In *Dalia v. United States*, the Supreme Court held that the manner in which law enforcement officials execute a warrant is subject to a Fourth Amendment standard of reasonableness. S. 1717 does not provide any more precise standard. Perhaps it would be impossible to provide a more precise standard and unwise to try. As it stands, the courts will have to consider the question as it arises, case-by-case.

Overall, then, S. 1717 fills two of the three significant shortcomings in title III. It merits passage.

THE
CATHOLIC UNIVERSITY
OF AMERICA
WASHINGTON D.C. 20064

THE COLUMBUS SCHOOL OF LAW
202 635-5140

March 5, 1980

To: The Senate Committee on the Judiciary
From: Clifford S. Fishman
Associate Professor of Law
Subject: S. 1717, a bill to amend certain provisions of
title 18, United States Code, relating to procedures
for interception of wire or oral communications.

Memorandum

This memorandum is submitted in the hopes that it will
prove useful to the Committee in analyzing S. 1717.

The Emergency Surveillance Provision

Section 5 of the proposal would amend 18 U.S.C. § 2518(7) by permitting interception of wire or oral communications without prior court approval in an emergency situation that "involves immediate danger of death or serious physical injury to any person."

18 U.S.C. § 2518(7) already permits emergency surveillance to investigate "conspiratorial activities threatening the national security interest or conspiratorial activities characteristic of organized crime." Within forty-eight hours of the initiation of the surveillance, an application must be submitted to a judge for an order retroactively approving the surveillance. The application must comply with all of the requirements set forth in Title III. If the application is denied, all evidence derived from intercepted communications is to be suppressed, and notice of the surveillance must be served in accordance with Title III.

The amendment should be enacted. If emergency surveillance is ever justified, certainly it is justified where there is probable cause to believe both that someone's life or safety is in immediate danger and that immediate interception of communications will provide evidence that might prevent the death or serious physical injury of the potential victim.¹ Such surveillance would be governed by all of the restrictions and requirements outlined in the previous paragraph; it is thus highly unlikely that law enforcement officials would make excessive and unjustified use of the provision.²

The proposal is firmly based on sound constitutional doctrine. Police officers are permitted to make a warrantless search and seizure of a premises where exigent circumstances exist that preclude postponement of the search until a warrant can be obtained.³ The proposal simply applies this principle of law in the context of electronic surveillance. Protection of human life and health is law enforcement's single most important function; currently, law enforcement officials might be precluded from taking necessary preventive action simply for lack of time to obtain prior judicial approval,⁴ even though the grounds and means for such action are apparent.

Entries Onto Premises

The bulk of the proposal deals with the issue of covert entry by law enforcement officials to implement a court order authorizing the interception of wire or oral communications.

Title III is silent on whether and under what circumstances covert entry is permitted to install a bugging device or wiretap. In Dalia v. United States,⁵ the Supreme Court held:

1. The Fourth Amendment does not prohibit covert entry per se.
2. Title III implicitly authorizes covert entry, since Congress must have been aware that such entry is sometimes necessary, particularly with regard to interception of oral communications.
3. The Fourth Amendment does not require that a Title III order contain a specific authorization to make covert entry. However, the majority, and dissenting Justices Brennan and Marshall, specifically endorsed current Justice Department policy of requesting specific authority for surreptitious entry.

4. Although the Fourth Amendment leaves it to the discretion of law enforcement officials to decide how a warrant is to be executed, the reasonableness of the execution is subject to judicial review at the suppression hearing.

The proposed legislation fills a significant void in Title III. It provides a broad and workable definition of "surreptitious entry," requires an interception application to state whether such entry is required and why, requires the order to expressly authorize such entry, and sets forth an appropriate standard by which the issuing judge is to measure the adequacy of the showing in the application.⁶ Likewise, it specifies the information which must be contained in the application and order. The proposal would usually require prior notice to the judge as to the time and method of entry, but permits the authorities to take immediate advantage of a fleeting opportunity; in the latter situation, the judge must be given a written statement of what was done and why within forty-eight hours of the entry.

In my opinion, the proposal merits enactment. Nevertheless, there are some aspects which may merit further clarification.

1. The proposal is silent as to whether an application for authority to make surreptitious entry must be authorized by the Attorney General or a specially designated Assistant Attorney General.⁷ Where the application seeks authorization to intercept oral communications by employment of a listening device, the need for surreptitious entry is apparent, and it is safe to presume that Attorney General authorization for such an application includes authorization to seek the right to make such entry. However, it may occasionally occur that the investigators discover the need to make surreptitious entry to install a wiretap only after the Attorney General has authorized the application. In such a case, should the applicant be required to obtain express authorization for surreptitious entry from the Attorney General? The policy reasons for requiring express Attorney General approval are apparent; on the other hand, such a requirement could delay the process considerably.

2. It may also arise that the need for surreptitious entry (e.g. to implement a wiretap) is discovered only after the judge has issued the interception order.⁸ In such a case, would it suffice for the attorney in charge to submit a supplemental affidavit requesting a supplemental order authorizing such entry; or would an entirely new application and order be required? A supplemental application and order should suffice, and it would be helpful for the final committee report to say so.

3. Notice to the judge. With regard to the initial entry, the attorney in charge must notify the judge in writing as to the "proposed time and method of entry."⁹ With regard to subsequent entries, the judge must receive a written statement of the reasons which necessitate the re-entry, but the proposal does not require that the judge be notified of the time and method.¹⁰ It seems worthwhile to require the attorney to notify the judge of the time and means of subsequent entry. Where practicable, the attorney should notify the judge of the proposed time and method when he submits the pre-re-entry statement of need. More often, exigencies may preclude prior notice, or might permit only prior notice of need but not prior notice of proposed time and method. In such situations, the written statement of time and method could be submitted to the judge within forty-eight hours of the re-entry.

4. "Method of entry." I take this phrase to mean the attorney in charge must inform the judge whether entry will be (or was) effected by a ruse or by a breaking (picking a lock, forcing a window, etc.). If more information than this is required, either the statute or the legislative history should say so.

5. Need the written notice to the judge explain the reasons that a particular method of entry has been chosen? The proposal is silent on this question, although it would be within the best interests of the government for the attorney in charge to include such an explanation in any event.¹¹

6. The judge's role. The proposal explicitly empowers the issuing judge to deny authority to make surreptitious entry if the need for such entry is not sufficiently established.¹² With regard to the particular method by which entry is to be or has been effected, however, the judge's role is not so clearly defined. If the judge receives prior notification, and disapproves of the method contemplated, has he the authority to prohibit use of that method? If so, what standard should the judge apply in deciding whether the method contemplated is appropriate? Can the government appeal the judge's decision not to allow the use of the contemplated method of entry? ¹³

Similarly, if the judge is not informed until after entry was effected, and disapproves of what was done, what sanctions may he impose? In *Dalia*, the Supreme Court held that the manner in which entry was effected is subject to subsequent judicial review, and that the basic issue is whether the method of entry was reasonable under the circumstances. Usually, of course, that issue would be litigated several months later, at an adversarial motion to suppress. If the issuing judge, informed after the fact of the method used, disapproves of what was done, has he the power to declare the method of entry unreasonable, to terminate the interception order, and to enter an ex parte order suppressing

the intercepted communications and any derivative evidence?¹⁴ This is certainly an unorthodox approach to suppression issues, and raises questions concerning whether the government has any recourse from an adverse ruling.¹⁵ The proposal's lack of specificity in this regard is even greater with regard to re-entries. As currently drafted, the proposal does not require the government to notify the judge of the methods that will be (or have been) used to re-enter the premises.¹⁶

The proposal appears to give the judge implicit authority to reject a proposed method or to condemn a method already used as unreasonable and as requiring an ex parte suppression order. Assuming this is the intent behind the proposal, it would be worthwhile to include in the Committee Report a statement that, given the government's lack of any practical opportunity to appeal such a suppression order, such authority should be exercised only in an extreme case.

6. Post-execution notice. The proposal does not require that those with a privacy interest in the premises ultimately be notified of the fact that surreptitious entry was effected, how often entry was made, or the methods used. It would be worthwhile to amend 18 U.S.C. § 2518(8)(d), the statutory inventory and notice provision,¹⁷ by adding a fourth subparagraph that requires such notice.

Respectfully submitted,

Clifford S. Fishman
Associate Professor of Law

NOTES

1. A Title III order may be issued only when, *inter alia*, the application establishes probable cause to believe, first, that a person is committing, has committed, or is about to commit a particular designated offense, and second, that interception of communications over the specified telephone or within the specified location will provide evidence of that offense. 18 U.S.C. § 2518(3) (a,b,d).

2. As a further check, 18 U.S.C. § 2518(7) requires such surveillance to be approved by the Attorney General. In addition, if the subsequent application for judicial approval is rejected or is not submitted, all those participating in the surveillance (including, presumably, the Attorney General), would be subject to potential civil liability pursuant to 18 U.S.C. § 2520.

3. See, e.g., *United States v. McKinney*, 477 F.2d 1184 (D.C. Cir. 1973); *Wayne v. United States*, 318 F.2d 205 (D.C. Cir. 1963) (Burger, J.); see generally 2 LaFare Search and Seizure 438-442, 455-458. Although the Supreme Court has not expressly so held, dictum in several cases appears to recognize the exigent circumstances exception. See *id.* at 432-438, 463-466; discussion of *Schmerber v. California*, 384 U.S. 757 (1966); *Chambers v. Maroney*, 399 U.S. 42 (1970); *Vale v. Louisiana*, 399 U.S. 30 (1970); *Williams v. United States*, 401 U.S. 646 (1971); *Mincey v. Arizona*, 98 S. Ct. 2408 (1978).

4. It could be argued that the organized crime provision of 18 U.S.C. § 2518(7) already provides authority for emergency surveillance in life-endangering situations. However, the undefined statutory phrase "characteristic of organized crime" is vague at best and may not apply to situations where the need for such surveillance is the greatest, e.g. a kidnapping for ransom by one or two individuals who are not acting for any "organization."

5. 60 L. Ed. 2d 177, 99 S. Ct. 1682 (1979).

6. Specifically, the proposal adopts the "ordinary procedures would be unavailing" standard contained in 18 U.S.C. § 2518(1) (c), (3) (c).

7. 18 U.S.C. § 2516(1) requires that the Attorney General or an Assistant Attorney General specially designated by the Attorney General authorize all federal Title III applications. Hereafter, the term Attorney General will be used to mean the Attorney General or a specially designated Assistant Attorney General.

8. This situation has arisen only rarely in the past. However, the 1978 amendment to 18 U.S.C. § 2511(2)(a)(ii) may make it more difficult for the government to obtain technical information from a telephone company prior to the issuance of the eavesdropping warrant. That section now apparently forbids a communications common carrier from providing any "information, facilities or technical assistance" to law enforcement officials for the purposes of executing a Title III warrant until after the carrier has been provided with a court order (or, in emergency situations, a written certificate of a high Justice Department official) directing the carrier to do so. Cooperation without such a court order exposes the carrier to civil liabilities. Hence, the agents may not learn of technical problems requiring entry until after the order is issued and the cooperation of a telephone company is sought.

9. Proposed addition of subsection 2518(4)(g)(ii), p. 4, lines 1-7. Normally such notice must be given to the judge prior to entry. If it is not practical to give prior notice, notice must be given within 28 hours after entry. *Id.*

10. Proposed new subsection 2518(4)(g)(iii), p. 4 lines 8-19.

11. See the next subtopic, *infra*.

12. See text accompanying note 6.

13. 18 U.S.C. § 2518(10)(b) affords the government the right to appeal the denial of an application for a Title III order, but does not address appeal of a decision by the issuing judge concerning the manner in which an order is executed after he has issued the order.

14. The legislative history of Title III indicates that the issuing judge is empowered to terminate surveillance if he becomes convinced that further surveillance is not necessary. Senate Report (Judiciary Committee) Number 1097, reprinted in 1968 U.S. Code Cong. & Admin. News 2193 (commenting on 18 U.S.C. § 2518(6), the "progress report" provision). By analogy, if the issuing judge concludes that the manner of covert entry was unreasonable, and that any interceptions or derivatives evidence are tainted and would be suppressed as lawfully obtained (see 18 USC § 2518(10)(a)(1)), termination of surveillance and ex parte suppression, although extreme sanctions, might be appropriate in an extraordinary case.

15. Concededly, the likelihood of termination and ex parte suppression is not great. Nevertheless, if the judge orders termination of surveillance, the government may be left without any remedy at all: by the time an appeal is heard, the probable cause which supported the application may be stale, the crimes under investigation may have already been committed, the targets of the investigation may have discovered the device, the period of surveillance authorized by the order may have expired, etc.

16. See text accompanying notes 11 & 12, *supra*.

17. 18 U.S.C. § 2518(8)(d) requires that an inventory must eventually be served on all those named in the order, and on other individuals as the judge sees fit, including (1) the fact that an eavesdropping warrant was issued, (2) the date of the warrant, and (3) the fact that communications were or were not intercepted.

Senator LEAHY. We will keep the record open for 2 weeks, and we will stand recessed until the call by the Chair.

Thank you.

[Whereupon, at 9:19 a.m., the hearing was adjourned.]

THE UNIVERSITY OF CHICAGO
LIBRARY
CHICAGO, ILL.

96TH CONGRESS
1ST SESSION

S. 1717

To amend certain provisions of title 18, United States Code, relating to the procedures for interception of wire or oral communications.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 5 (legislative day, JUNE 21), 1979

Mr. KENNEDY introduced the following bill; which was read twice and referred to the Committee on the Judiciary

A BILL

To amend certain provisions of title 18, United States Code, relating to the procedures for interception of wire or oral communications.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 That section 2510 of title 18, United States Code, is
4 amended—

5 (1) in paragraph (10), by striking out “and” at the
6 end thereof;

1 (2) in paragraph (11), by striking out the period at
2 the end thereof and inserting in lieu thereof a semi-
3 colon and "and"; and

4 (3) by adding at the end thereof the following:

5 “(12) ‘surreptitious entry’ means a physical entry
6 upon a private place or premises to install, repair, re-
7 position, replace, or remove any electronic, mechanical,
8 or other device, and includes both covert entry and
9 entry effected by means of a ruse or subterfuge.”.

10 SEC. 2. Section 2518(1) of that title is amended—

11 (1) in paragraph (e), by striking out “and” at the
12 end thereof;

13 (2) in paragraph (f), by striking out the period at
14 the end thereof and inserting in lieu thereof a semi-
15 colon and “and”; and

16 (3) by adding at the end thereof the following:

17 “(g) a statement whether surreptitious entry is re-
18 quired to effect the interception, and if such surrepti-
19 tious entry is required, a statement as to why means of
20 effecting the interception other than surreptitious entry
21 reasonably appear, if tried, to be unlikely to succeed,
22 to be too dangerous, or to be impracticable.”.

23 SEC. 3. Section 2518(3) of that title is amended—

1 (1) in paragraph (d), by striking out the period at
2 the end thereof and inserting in lieu thereof a semi-
3 colon and "and"; and

4 (2) by adding at the end thereof the following:

5 “(e) where the order is to authorize or approve a
6 surreptitious entry, such surreptitious entry reasonably
7 appears to be required to effect the interception be-
8 cause means of effecting the interception other than
9 surreptitious entry reasonably appear, if tried, to be
10 unlikely to succeed, to be too dangerous, or to be
11 impracticable.”.

12 SEC. 4. Section 2518(4) of that title is amended—

13 (1) in paragraph (d), by striking out the “and” at
14 the end thereof;

15 (2) in paragraph (e), by striking out the period at
16 the end thereof and inserting in lieu thereof a semi-
17 colon and “and”; and

18 (3) by adding at the end thereof the following:

19 “(f) whether surreptitious entry is authorized or
20 approved to effect the interception; and

21 “(g) in any order which includes authorization of
22 surreptitious entry—

23 “(i) the identity of the agency authorized to
24 make the surreptitious entry;

1 “(ii) that the attorney for the government in
2 charge of the investigation shall, when practica-
3 ble, notify in writing the authorizing judge of the
4 proposed time and method of the entry, and when
5 prior notice is not practicable, notification is to be
6 made within forty-eight hours after such entry;
7 and

8 “(iii) that in any case in which more than
9 one entry is necessary to install the device, or in
10 which reentry is necessary to repair, reposition, or
11 replace the device, the attorney for the govern-
12 ment in charge of the investigation shall, when
13 practicable, notify in writing the authorizing judge
14 prior to such reentry of the reasons which neces-
15 sitate the reentry, and when prior notice is not
16 practicable, such notification is to be made within
17 forty-eight hours after the reentry and is to de-
18 scribe the reasons which necessitated the reentry
19 and why prior notification was not practicable.”.

20 SEC. 5. Section 2518(7) of that title is amended—

21 (1) by amending paragraph (a) to read as follows:

22 “(a) an emergency situation exists that involves—

23 “(i) immediate danger of death or serious
24 physical injury to any person,

5

1 “(ii) conspiratorial activities threatening the
2 national security interest, or

3 “(iii) conspiratorial activities characteristic of
4 organized crime,

5 that requires a wire or oral communication to be inter-
6 cepted before an order authorizing such interception
7 can, with due diligence, be obtained, and”; and

8 (2) by inserting a comma and “and may make any
9 surreptitious entry required to effect such intercep-
10 tion,” immediately before “if an application for an
11 order”.

12 SEC. 6. Section 2519(1) of that title is amended—

13 (1) by inserting immediately after paragraph (e)
14 the following:

15 “(f) the fact that a surreptitious entry to effect the
16 interception was authorized or approved, the number of
17 such entries made, and the purpose, either to install,
18 repair, reposition, replace, or remove the interception
19 device, for each such entry;”; and

20 (2) by redesignating paragraphs (f) and (g) as
21 paragraphs (g) and (h), respectively.

22 SEC. 7. Section 2519(2) of that title is amended in para-
23 graph (a) by striking out “(g)” and by inserting in lieu thereof
24 “(h)”.

96TH CONGRESS
1ST SESSION

S. 1815

To require explicit authorization from judges of competent jurisdiction for any covert entry onto premises for the purpose of installing and removing any electronic interception devices to be utilized in the investigation of specified criminal offenses.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 25 (legislative day, JUNE 21), 1979

Mr. NELSON introduced the following bill; which was read twice and referred to the Committee on the Judiciary

A BILL

To require explicit authorization from judges of competent jurisdiction for any covert entry onto premises for the purpose of installing and removing any electronic interception devices to be utilized in the investigation of specified criminal offenses.

- 1 *Be it enacted by the Senate and House of Representa-*
- 2 *tives of the United States of America in Congress assembled,*
- 3 That this Act may be cited as the "Omnibus Crime Control
- 4 and Safe Streets Act Amendments of 1979".

1 SEC. 2. Section 2518(1) of title 18, United States Code,
2 shall be amended by adding a new subsection (g), which shall
3 read:

4 “(g) a statement of whether or not a covert
5 method of entry into private premises for the purposes
6 of installing and removing any electronic interception
7 device(s) is to be utilized in accomplishing any oral in-
8 terception otherwise allowable under this chapter. Such
9 statement shall also contain the reasons why illegal
10 entry as opposed to legal methods of entry must be
11 employed.”.

12 SEC. 3. Section 2518(4) of title 18, United States Code,
13 shall be amended by adding a new subsection (f), which shall
14 read:

15 “(f) whether or not a covert method of entry for
16 the purposes of installing and removing any electronic
17 interception device(s) is to be utilized in accomplishing
18 any oral interception otherwise allowable under this
19 chapter.”.

20 SEC. 4. Section 2518(4) of title 18, United States Code,
21 shall be amended by adding after new subsection (f):

22 “Judges of competent jurisdiction shall not grant requests to
23 employ a covert method of entry into private premises for the
24 purposes of installing and removing any electronic intercep-
25 tion device(s) without also stating in the order permitting

1 such interception the reasons why legal methods of entry
2 would appear to be unlikely to succeed if tried or would be
3 too dangerous to the officers attempting to install the
4 interception device.”.

Prepared Statement of H. Stuart Knight, Director
 Representing: United States Secret Service
 1800 G Street, NW
 Washington, DC 20223

March 5, 1980

Mr. Chairman and members of the Committee:

On behalf of the Secret Service, I would like to take this opportunity to comment on Senate Bill 1717, proposing amendments to Section 2518 of Title 18, United States Code "Procedure for Interception of Wire or Oral Communications." I have specifically been requested to provide a scenerio as to how the U.S. Secret Service might utilize the authority under the proposed amendments.

Under Section 3056 of Title 18, United States Code, the U.S. Secret Service has a two-fold responsibility; personal protection of the President and criminal investigation of laws as they pertain to maintaining the integrity of U.S. currency. There are occasions under both when the proposed amendments would be beneficial.

Obviously, the most significant advantage would be in protecting the life of the President of the United States. The current provisions of Section 2518, paragraph 7-a, provide for emergency interception of wire or oral communication when "an emergency situation exists with respect to conspiratorial activities threatening the national security interest . . .". This would encompass the life of the President.

In a situation where a conspiracy against the life of the President was discovered hours or even one or two days prior to the arrival of the President and only a single suspect has been identified, these provisions might apply. Although physical surveillance of that single suspect could preclude adverse action on his part, wire interception of the suspect's telephone and/or oral interceptions from his residence could determine the scope of the conspiracy and assist in identifying others involved, thus neutralizing the threat.

A second situation in which the proposed amendments would be extremely beneficial is very similar to the first but with the target of the assassination a protectee other than the President. The U. S. Secret Service protects presidential family members, the Vice President, members of his family, foreign heads of state and heads of government, and Presidential candidates and nominees. The proposed amendment to paragraph 7, subsection (a-i) which includes as an emergency situation an immediate danger of death or serious physical injury to a person, would allow the same measures to be taken when any of these are threatened as with the President.

If the unfortunate occurred and any protectee was taken hostage, the ability to rapidly place into operation the interception of wire communications from the hostage site as well as devices to monitor oral communications from within could be of immeasurable benefit. Again, the proposed benefits would be of the most use in the case where the hostage was other than the President and fell outside the "National Security" umbrella.

The use of an emergency interception that also involves surreptitious means to protect life would also be a useful tool in our criminal investigations. The use of undercover agents to deal with criminal elements is a primary investigative technique in the suppression of counterfeit printing plants. Should the status of an undercover agent be compromised and the agent be taken hostage, the same benefits would be derived as with the other hostage situation.

The proposed amendments concerning surreptitious entry for Title III electronic surveillance would formalize prior judicial review of the reasonableness of the covert entry as well as the interception itself. Since in current practice an approving judge would be aware of the need for surreptitious entry, we see no problems arising from this change. The authority to make surreptitious entries is necessary to effect electronic surveillance of such places as the meeting sites of conspirators.

The amendments as proposed would not necessarily be used on a routine or frequent basis. They would, however, provide valuable tools for use in those situations of the most severe nature.

Prepared Statement of Kenneth J. Hodson
Representing the American Bar Association

Mr. Chairman, my name is Kenneth J. Hodson. As Chairman of the American Bar Association Standing Committee on Association Standards for Criminal Justice, I am pleased to have been asked to present the views of the American Bar Association on proposed amendments to Title 18, United States Code, represented by S. 1717.

The Association policy positions which I will articulate in support of these amendments are contained in the American Bar Association Standards for Criminal Justice Relating to Electronic Surveillance. These Standards were drafted by the Association over a ten-year period (from 1963-1973) as an expression of Association leadership in the criminal law revolution of the 1960's. They were designed to give criminal justice planners, legislators, courts, practitioners, and the lay public an understandable and constitutionally supportable set of guidelines. Thus, they were intended to serve as suggested procedures for overhauling, reforming, and strengthening the criminal justice system to enable it to respond to current and foreseeable demands. Above all, they were intended to assist in bringing about a much-needed balance between the interests and security of society and the rights of the accused. Chief Justice Warren E. Burger has described these standards as the "single most comprehensive and probably the most monumental undertaking in the field of criminal justice ever attempted by the American legal profession in our national history."

The original Standards project produced 18 sets of Standards spanning the spectrum of the criminal justice process from the police function through final postconviction procedures. The set of Standards Relating to Electronic Surveillance was one of the 18, and its first edition

received approval of the American Bar Association's governing House of Delegates in 1971.

I think it would be helpful to the Subcommittee if I capsulized the methodology utilized in producing the ABA Standards for Criminal Justice. The Standards formulation process was an intensive undertaking which was designed to thoroughly examine the problem; to address it in terms of the applicable constitutional provisions, case and statutory law, procedural rules, and existing practices; and to assess the accumulated experience as exemplified by actual practice and its impact on the system, the accused, society, and the government. Out of that effort, the project was designed to formulate Standards - richly documented by historical background, proven practice, and sound rationale - which would constitute the recommended procedures covering the subject area.

A Special Committee on Standards for the Administration of Criminal Justice served as the parent oversight group for the entire undertaking. It was responsible for setting policy, articulating procedures, establishing lines of accountability, and ensuring coordination and communication. The Committee was appointed by the Association's President from among its 250,000 members, and comprised a balanced representation of the judiciary, prosecution, and defense. Its first Chairman was The Honorable J. Edward Lumbard, then Chief Judge of the U.S. Court of Appeals for the Second Circuit. He served from 1963 until 1968, when he was succeeded by then United States Court of Appeals Judge Warren E. Burger who remained until his confirmation as Chief Justice of the United States in 1969, when the chairmanship passed to United States District Court Judge William J. Jameson, of Montana, a former President of the ABA. The current and incoming heads of the

Section of Criminal Justice and Judicial Administration Division served as ex-officio members. In turn, the Special Committee appointed task forces of experts in all aspects of the assigned subject areas. Each was supported by one or more consultant/reporters, selected because of special substantive expertise, research and writing skills. The task forces and consultant/reporters were responsible for preparing the initial drafts. Their drafts were then thoroughly reviewed, debated, remanded for any necessary clarification or changes, and ultimately cleared by the Special Committee. The Special Committee's considerations were augmented by valuable input from liaison representatives of various other groups invited by it to participate.

When the Special Committee had ultimately finalized a tentative draft, it was printed and circulated widely for comment from a large number of ABA entities and outside groups. In some instances as many as 13,000-17,000 copies of a tentative draft were disseminated for comment. Following receipt and thorough consideration of all feedback, the tentative draft was finalized for presentation to the ABA Board of Governors for clearance to be placed on the agenda of the House of Delegates. Here the draft was debated, in some instances amended, and ultimately approved by the Association. At that point the approved Standards became official Association policy, ready for publication and nationwide dissemination. This thorough methodology which was tested in formulating the First Edition, and thereafter proven in years of nationwide implementation, has become a hallmark of the Standards.

Because of the widespread acceptance and use of the Standards at federal, state, and local levels, the Association created the Standing Committee which I now Chair to serve as a continuing monitor for them. One of its assigned responsibilities is the task of keeping the Standards up to date in response to court decisions, legislation resulting from developments in such a dynamic area as criminal justice, and feedback from the Association's extensive implementation efforts. In 1979 the Standing Committee completed an almost three-year project of reevaluating and making any necessary revisions in the Standards. Each of the Standards was subjected to the same painstaking process as was followed in formulating the First Edition.

The Second Edition of Electronic Surveillance Standards was approved by the House of Delegates August 9, 1978. I am pleased to report that the Second Edition is substantially unchanged from its initial version. The First Edition was being formulated when the Congress was considering Title III of the Omnibus Crime Control and Safe Streets Act of 1968, and when the House of Delegates approved them in February 1971, Title III had been enacted (P.L. 90-351). There was substantial similarity between the two.

The Electronic Surveillance Standards and Title III have withstood constitutional and other challenges in the intervening years. Significantly, the National Wiretapping Commission, for which I was privileged to serve as Executive Director, evaluated the effectiveness of Title III. Its report of April 1976 to the President and the Congress supported the overall effectiveness of Title III in constitutionally and reasonably protecting conversational privacy, as well as providing a useful investigatory tool for law enforcement in

coping with organized crime and conspiratorial activities.

With the foregoing as a backdrop, let me now address the specific amendments to Title III proposed by S. 1717. The American Bar Association is pleased wholeheartedly to support both the letter and spirit of the amendments. They are in accord with the spirit of the Electronic Surveillance Standards as first promulgated, and as reinforced by the Second Edition.

Let me first address the proposed amendment to Section 2518(7) which would authorize emergency interception in a situation which "involves immediate danger of death or serious physical injury to any person," and also would authorize making "any surreptitious entry required to effect such interception" upon a reasonable determination that grounds exist upon which a court order could be obtained. It is noted that all other existing requirements would apply, including the making of an application within 48 hours after the interception begins or has occurred, the making of recordings, placing them in the judge's custody for sealing, the statutory inventory requirements, etc.

The Second Edition of Electronic Surveillance Standards was amended expressly to extend emergency surveillance authority to situations "involving substantial and imminent danger to human life." (ABA Standards for Criminal Justice, Standard 2-5.2(i), 1978) The commentary supporting this ABA Standard refers to "risk of serious injury or death" which would equate the ABA intended coverage with that of S. 1717. Although the intention was to make explicit what had been implicit in the First Edition, an additional objective was clearly to take cognizance of an increasing incidence of crimes involving serious and imminent life-threatening

situations - such as kidnappings, terrorism, hostage holdings and certain other organized or conspiratorial activities. More often than not, the very nature of these incidents would not permit time for first filing the application and obtaining a court order. Consistent with the provisions of Title III, the ABA Standards would impose all other non-emergency court-approved requirements of recording, return, and inventory. Also, every emergency surveillance would have to be based on a law enforcement/prosecutorial determination that grounds exist which would support a pre-authorized court order, and a regular application for court approval, including facts to justify the emergency must be filed not more than 48 hours after institution of the surveillance. (ABA Standards for Criminal Justice, Standards 2-5.2(a)(ii), (iii), 2-5.2(b), 1978)

I now refer to the second proposed amendment to Section 2518(7), intended to authorize surreptitious entry in emergency interceptions, provided grounds exist which would have justified a court order for such. The ABA Standards, while not explicit on this point, would permit surreptitious entry in an emergency situation by authorizing emergency surveillance when

[T]he law enforcement officer, specially designated by the appropriate prosecuting officer as described in Standard 2-1.1(c): . . . (ii) determines that there are grounds consistent with these standards upon which an order could be obtained authorizing such an overhearing. . . . (ABA Standards for Criminal Justice, Standard 2-5.2(a)(ii), 1978)

As I shall explain later in this statement, the ABA Standards permit surreptitious entry in cases meeting the requirements for court-ordered surveillance. Thus, it follows that surreptitious entry would be permitted in appropriate cases meeting the requirements for emergency surveillance.

The requirements for court-ordered surveillance are enumerated in explicit detail in Standard 2-5.3, and require, among other things, the following:

(v) a particular description of the type of communications sought to be or which were overheard or recorded; (vi) a particular description and the location of the facilities, if any, over which or the place where the communications are to be or were overheard or recorded. . . . (viii) a complete statement of the facts relied upon by the applicant warranting the issuance of an order of authorization or approval; (ix) a full and complete statement of other investigative procedures that have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous. . . . (ABA Standards for Criminal Justice, Standard 2-5.3(v), (vi), (viii), (ix), 1978)

It should be noted that the First Edition of these Standards was cited by the majority opinion in Dalia v. United States, 99 S.Ct. 1682(1979) as recognizing the need for surreptitious physical entry when "bugs" are installed and removed. Therefore, the American Bar Association supports this amendment because it will serve to remove any doubt as to the intent of the Congress.

Finally, I would like to comment on the remaining group of amendments in S. 1717, addressing them individually.

The first is the proposed definition of "surreptitious entry" which would be included in Section 2510. I feel this is entirely adequate, for it includes physical entries which might be effected either by pretext or covertly. The ABA Standards contain no counterpart, but rather rely on the requirement that the application for an order contain facts applicable to each specific case, which would cover the type of communications to be surveilled, the precise location and description of the facilities or place, and a justification of need for the type of electronic installation sought. (See ABA Standards for Criminal Justice, Standard 2-5.3, 1978) Considering the

fact that standards are not intended to be as precise as legislation, but are designed to set forth principles to serve as guidelines for a variety of implementation options, we certainly endorse the wisdom of including an explicit definition in Title III.

The second proposed amendment pertains to Section 2518(1). It requires any application for an order authorizing or approving the interception of a wire or oral communication expressly to state whether surreptitious entry is required; and if so, to explain why less intrusive means "reasonably appear, if tried, to be unlikely to succeed, to be too dangerous, or to be impracticable."

The ABA Standards agree in principle with this proposed amendment, as previously indicated. Again, we endorse the desirability of legislation being more precise and explicit than the Standards, and that appears to have been accomplished in this instance. I have no questions or suggested changes. However, I note the statement of Senator Edward M. Kennedy that "It is not the purpose of these amendments to preclude the use of surreptitious entries for at times they are the only practical means of installing a court-authorized surveillance device which will produce evidence of a serious crime." Not only do I agree with that assessment, but I also agree with Assistant Attorney General Philip B. Heymann, who testified that the section-by-section analysis of the bill supports the intention that where the interception of oral communications is approved, no extraordinary showing of necessity for surreptitious entry is mandated. The American Bar Association also agrees with the Federal Bureau of Investigation that a very weighty factor in evaluating necessity for surreptitious entry is the personal safety of the law enforcement personnel.

The third proposed amendment applies to Section 2518(4). It would require the judge to specify in each order whether surreptitious entry is authorized; and to include requirements for keeping the judge informed of the proposed time and method of entry, and reasons for any reentries.

Again, the ABA Standards do not spell out these precise requirements for the court order. However, Standard 2-5.8 which covers the order, form, and contents, provides that the order should contain, inter alia, the following:

(v) a particular description of the type of communications sought to be or which were overheard or recorded; (vi) a particular description of and the location of the facilities from which or the place where the communications are to be or were overheard or recorded. . . . (ABA Standards for Criminal Justice, Standard 2-5.8, 1978)

The commentary to Standard 2-5.8 specifically indicates that the surveillance order is intended to contain "the judge's instructions, guidelines, and controls," and "like conventional search warrants, should be inclusive." The order should not rely on incorporating the application by mere reference, because applications are only the request for authority, and also are frequently long and contain irrelevant material. Thus, it logically follows that the American Bar Association would endorse the particularity required in S. 1717.

We believe the requirements pose no unreasonable burden on the judge or the applicant. Again, I take note of the testimony of Mr. Heymann on behalf of the Department of Justice and Executive Assistant Director Lee Colwell of the Federal Bureau of Investigation, and agree wholeheartedly that the intended flexibility in Section 2518(4) be retained so as not to unreasonably hamstring enforcement in confronting unforeseen on-the-site circumstances which may require a change in time or method of entry or

additional entries to adjust or repair equipment, but require notice of such within 48 hours when prior written notice in such cases is not possible. Equally important, I feel, is a reasonable interpretation of the requirement for notice of method of surreptitious entry, so as not to compromise essential security of investigative techniques and technology or risk potentially dangerous disclosure of cooperative persons. The American Bar Association gave these critical factors long and thoughtful deliberation in drafting and updating its Standards. We firmly believe that Title III, as amended, will enable the judge to obtain all the information needed to discharge his or her responsibility, and yet not unreasonably about the increasingly heavy reliance society places on law enforcement.

In conclusion, Mr. Chairman, I can confidently state that all of the amendments proposed in S. 1717 would make explicit what has, in our opinion, been implicit in the ABA Standards Relating to Electronic Surveillance. We have heretofore been confident that Title III was a legislative embodiment of the principles in the Standards which are addressed by S. 1717. Our position was vindicated by the majority opinion in Dalia v. United States (supra). However, by enactment of these amendments, the Congress will also be accommodating the footnote comment of the majority view in Dalia as follows:

Although explicit authorization of the entry is not constitutionally required, we do agree with the Court of Appeals that the "preferable approach" would be for Government agents in the future to make explicit to the authorizing court their expectation that some form of surreptitious entry will be required to carry out the surveillance. Indeed, the Solicitor General has informed us that the Department of Justice has adopted a policy requiring its officers, "to include [in applications for Title III orders] a request that the order providing for the interception specifically authorize surreptitious entry for the purpose of installing and removing any electronic interception devices to be utilized in accomplishing the oral interception." (99 S.Ct. 1682, fn 22, at 1694)

Mr. Chairman, I appreciate the opportunity which you have given the American Bar Association to articulate its views on this important legislation. I shall be pleased to respond to any questions or request for supplemental information which the Subcommittee may desire.



UNITED STATES DEPARTMENT OF JUSTICE
DRUG ENFORCEMENT ADMINISTRATION
Washington, D.C. 20537

FEB 29 1980

The Honorable
Patrick J. Leahy
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Senator Leahy:

I appreciate your kind invitation to present to the Subcommittee on Criminal Justice the views of the Drug Enforcement Administration regarding S. 1717, legislation that would amend the current wiretap law. By way of this letter, I would like to submit the following for the record.

At the outset, I would like to associate myself with the comments of the Department of Justice, which were submitted to the Vice President on August 9, 1979. The intent of this legislative proposal is clear. It is designed, in part, to provide procedural safeguards to insure informed judicial consideration of the need for and the reasonableness of surreptitious entry to effect an interception under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 USC 2510 et seq.). The balance of S. 1717 is concerned with amending present law to provide an additional circumstance under which an emergency interception may be authorized; that is, in the event there is a situation in which there is an immediate danger of death or serious physical injury to any person.

Although the Supreme Court, in United States v. Dalia held that, "the Fourth Amendment does not require that a Title III electronic surveillance order include a specific authorization to enter covertly the premises described in the order" (99 S. Ct. 1694 (1979)), it also commented that the "preferable approach" was for the government agents to make explicit to the court their expectation that surreptitious entry would be required to effect the interception. The court further noted its approval of the Department of Justice's current regulation regarding this point.

I believe that it is a well-considered policy to require judicial involvement in this process. The issue here concerns the balance of the needs of law enforcement and the citizen's reasonable

expectations of privacy. With respect to surreptitious entry to install the means of a Title III interception, the citizen's rights are two-fold. Not only does a citizen have an expectation of privacy of conversation, he also expects physical privacy. These unique privacy considerations make judicial scrutiny appropriate, in as much as in this instance, it is not designed to preclude the use of surreptitious entry, but rather to subject such entry to the approval of an impartial judicial officer. In this manner, the aforementioned delicate balance can be maintained.

The proposed amendment provides the judge with advance notice that a surreptitious entry is anticipated and also provides him with sufficient information to determine whether such entry is reasonable. The applicant needs to demonstrate that surreptitious entry is being sought because other methods of interception would most likely be too dangerous, impracticable, or would not succeed.

As a rule, implementation of a wire intercept does not require surreptitious entry. It is generally accepted that the only effective method of intercepting oral communications is through the installation of a concealed surveillance device and, consequently, surreptitious entry is most often required. Because the majority of the sections of this legislative proposal are directed at oral interceptions, they will not affect DEA's operations to any great extent. The following breakdown clearly shows that DEA has not conducted an oral intercept for over two years.

CY 1976	26 wire 2 oral
CY 1977	15 wire 7 oral
CY 1978	20 wire 0 oral
CY 1979	11 wire 0 oral

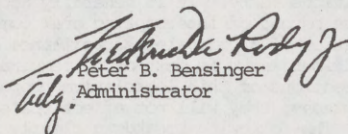
In each instance that an oral intercept was utilized, Department of Justice authority and a court order were obtained.

The only section in S. 1717 which gives me any cause for concern is Section 4, which provides that the interception order shall identify the agency authorized to make the entry and shall propose the time

and method by which the entry shall be conducted. Most importantly, I believe that such notification should be made only in the most general terms that would be acceptable to the court. For example, I would assume as far as time is concerned that language such as "on or about May 15" or "during the week of May 11" would be acceptable. I am likewise concerned that the language of the bill may prompt the issuing judge to require detailed explanations of the methods by which access is to be obtained. Such details could ultimately result in the relatively few sensitive methods of entry being made public and thus give the criminal element further insight into law enforcement's operations. I recognize that and approve of the fact that such notification does not preclude the officers executing the order from making last minute changes if the circumstances warrant.

In summary, I believe that S. 1717 is a most reasonable proposal, one that does not hinder the efforts of the law enforcement community and yet provides privacy safeguards for the citizen.

Sincerely,


Peter B. Bensinger
Administrator



DEPARTMENT OF THE TREASURY
BUREAU OF ALCOHOL, TOBACCO AND FIREARMS
WASHINGTON, D.C. 20226

Honorable Patrick J. Leahy
United States Senate
Washington, DC 20510

Dear Senator Leahy:

This is in response to your request for ATF's comments on S. 1717.

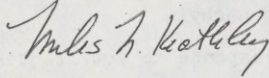
The proposed legislation would amend Title III of the Omnibus Crime Control and Safe Streets Act of 1968, to address two issues in connection with the interception of wire or oral communication for law enforcement purposes: the use of a surreptitious entry to effect an interception under Title III and authority to conduct emergency interceptions without prior court approval in situations which involve immediate danger of death or serious physical injury to a person.

As we interpret the amendment, the provision that addresses surreptitious entry to effect a court ordered interception under Title III would require further judicial approval of a surreptitious entry to intercept a communication. We understand that this amendment is intended to supersede the decision of the Supreme Court in *Dalia v. United States*, 99 S. Ct. 1682 (1979), which held that implicit in an order authorizing the interception of oral communications is the authority to make a surreptitious entry. The second purpose of the bill is to provide statutory authority for an emergency interception of communications in life-threatening situations without the necessity of a court order.

The procedural mandates of the bill requiring prior judicial review of a surreptitious entry would not in our view hamper ATF in the undertaking of its law enforcement responsibilities. In this connection, we would point out that ATF's records reflect only one instance in which an interception of communications was initiated under Title III. Therefore, we do not believe that the requirement for judicial review in these circumstances would be particularly burdensome.

The bill's expansion of Title III to provide authority to intercept wire or oral communications in emergency situations is in our view a beneficial provision which could be extremely useful in our criminal investigations. ATF has the authority to intercept communications under Title III in connection with its enforcement of Federal explosives laws under 18 U.S.C. § 844 which proscribes criminal misuses of explosives. Although we cannot cite an instance in the past where to our knowledge an immediate interception in an emergency situation might have prevented death or bodily harm, cases arising under our explosives jurisdiction have the potential for use of such emergency interceptions.

Sincerely yours,

A handwritten signature in cursive script, reading "Miles H. Keithley".

Acting Director

AMERICAN CIVIL LIBERTIES UNION

Washington Office

March 26, 1980

The Hon. Patrick J. Leahy
United States Senate
Washington, D.C. 20510

Dear Senator Leahy:

In response to your invitation to the American Civil Liberties Union to set forth its views on S. 1717, a bill relating to procedures for interception of wire or oral communications, we are submitting the following comments.

S. 1717 establishes certain procedural safeguards to insure informed judicial consideration of the need for and the reasonableness of surreptitious entry in the placement of microphone eavesdropping devices authorized under Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The legislation is intended to address the issue created by the Supreme Court's recent decision in *Dalia v. United States*, _____ U.S. _____, 99 S.Ct. 1682 (1979), which held that such safeguards are mandated neither by the Constitution nor by statute. In this respect the legislation is a clear improvement over current law and investigative practice, in that it requires separate judicial scrutiny of the particular means to be employed to initiate microphone electronic surveillance and thereby strengthens the warrant procedure authorized under Title III. To the extent that this enhances the protection of Fourth Amendment interests, the American Civil Liberties Union endorses the bill.

Despite our endorsement of S. 1717, however, we wish to make it clear for the record that we oppose the use of electronic surveillance--whether by microphone or wiretap--because its sweep, unlike the sweep of physical searches, inevitably intrudes far beyond any particular incriminating conversations. Taps and bugs necessarily record all communications during the period of authorized surveillance. Moreover, their demonstrated utility for law enforcement purposes is questionable, and their cost to individual privacy outweighs their benefit.

We wish to state for the record that we believe the authority to install microphone eavesdrops should be repealed or substantially narrowed.

First, such surveillances are far more intensive than wiretaps, for they reach everyone in the room or house bugged, and it is impossible to fulfill the minimization requirements. Second, it is virtually impossible to install bugs without a surreptitious entry, thus violating the sanctity of the home or other target area and thereby doubly violating individual rights. Third, there are indications that bugs are even less successful than the none-too-successful wiretaps. Studies of federal telephone wiretapping show that the number of convictions is about twice the number of taps and bugs (1826 convictions for 864 taps and bugs in 1973 as of December 31, 1978, according to the Administrative Office of the U.S. Courts). More pertinently, only ^{1/} about a third of the intercepts are associated with convictions. This is bad enough, but for bugs, it appears much worse, as the following analysis shows.

According to figures provided by the Administrative Office of the U.S. Courts, most microphone eavesdrops (m/e's) are installed as part of a package with wiretaps. In order to determine what convictions are associated with m/e's alone, it is necessary to check those intercepts where only an m/e was involved. There were 79 such federal bugs during 1969-78, 43 of them from 1973-76. Since it usually takes about 2 years for the results to come in on a bug, we should by now have a reasonably good test of the effectiveness of these 43. Analysis of these 43, which account for more than a half of the total through 1976 and are therefore a good sample, shows that:

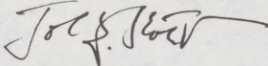
- (1) There have been only 37 convictions in cases where the bugs were used, compared with the overall 2:1 ratio for taps and bugs together (the overwhelming bulk of which are of course phone taps);
- (2) Only 9 of the 43 intercepts are directly associated with a conviction, a 21% percentage, in contrast with the 33% for both taps and bugs;
- (3) Of the convictions associated with bugs, most are for gambling, contempt, perjury and the like--1 Florida bug listed as "espionage" and associated with 3 convictions (i) turned out to actually involve convictions for violation of the Export Administration and Alien Registration Acts and (ii) the convictions were reversed by the Fifth Circuit Court last fall (U.S. v. Heiser).

^{1/} Whether there is actually a causal link between the tap and the conviction is not revealed by the statistics; qualitative evidence on specific intercepts and cases indicates there is not. See, H. Schwartz, Testimony for the National Wiretap Commission, 2 Hearings 1088, 1130 (Table 9) (1974).

The average bug, according to the Administrative Office, cost \$23,000 in 1978 (not including many auxiliary costs such as lawyers' and judges' time preparing papers, etc.), less than the average 1978 intercept (\$27,000), but that is because many bugs are in for just a few days, or do not work. Some individual bug installations cost more than the average, some reaching as high as \$70,000 (again, excluding auxiliary costs).

For all these reasons, the ACLU endorses the new procedural protections in S. 1717, but urges the Committee to approve this bill as a first step toward reconsidering the statutory authorization of microphone surveillance. The cost to privacy is too high to justify the limited benefits obtained from this intrusive investigative practice.

Yours sincerely,

A handwritten signature in dark ink, appearing to read "John H.F. Shattuck", with a stylized, flowing script.

John H.F. Shattuck
Director

THE
CATHOLIC UNIVERSITY
OF AMERICA
WASHINGTON D.C. 20064

THE COLUMBUS SCHOOL OF LAW
202 635-5140

March 18, 1980

Senator Patrick J. Leahy
United States Senate,
Committee on the Judiciary
232 Russell Senate Office Building
Washington, D.C. 20510

Re: S. 1717

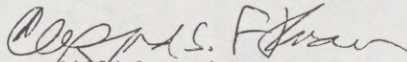
Dear Senator Leahy:

Thank you for giving me the opportunity to testify
on S. 1717.

My comments on your additional questions are attached.
S. 1717 corrects two of the three significant shortcomings
in Title III of the Omnibus Crime Control and Safe Streets
Act of 1968. It merits passage. Still, there are aspects
of the bill that could be improved or clarified, particularly
with regard to the reentry provision (question 2), the issue
of pre-trial discovery (question 3), and how the reasonable-
ness of the method of entry should be measured (question 7).

I would welcome an opportunity to be of further service.

Very truly yours,


Clifford S. Fishman
Associate of Law

Enclosure

CSF:mf

Questions of Senator Leahy and Responses
of Professor Fishman

Question 1. Since the Supreme Court in Dalia has held that a covert entry provision is not a required part of a Title III order, what benefit do you see flowing from this legislation?

The surreptitious entry provisions of S.1717 codify current Justice Department practice and may serve as a model for state legislation. The bill provides a broad, workable definition of surreptitious entry, specifies the showing that the application must make before such entry may be authorized, sets forth an appropriate standard against which this showing is to be measured, and requires that the intercept order explicitly authorize entry.

Thus, S. 1717 imposes a greater measure of judicial control over surreptitious entry than currently exists.

Question 2. In some instances, it is necessary for the agents who are installing a Title III intercept device to re-enter the premises to repair, replace or reposition the device. Does this legislation adequately provide for those situations or should the entry provision specifically provide for such re-entries?

Section 4 regulates reentries. Two aspects of this section might be improved upon.

First, section 4 does not regulate reentry to remove the device after interception has terminated.. Reentry to remove should be regulated in the same way as any other reentry. I suggest the following amendment:

- a. Page 4 line 10: delete "or"
- b. Page 4 line 11: insert a comma and the words "or remove" after the word "replace" .

Second, section 4 appears to treat reentries differently from the initial entry. The government attorney must notify the issuing judge of the time and method of the initial entry. The reentry provision, however, appears to require only that the government attorney notify the judge of the necessity for reentry.

There is no reason why reentries should not be subject to the same judicial oversight as is the initial entry. Hence, I suggest the following amendments:

- a. Page 4 line 14: insert, after "of the" , the words "proposed time and method of the reentry and the" ;
- b. Page 4 line 18: insert, after the first "the", the words "time and method of the reentry and the" .

Question 3. The FBI and DEA have pointed out that notification of the time and method of entry may jeopardize subsequent use of the same methods in other cases. Do you have any comment about these concerns?

In *Dalia v. United States*, the Supreme Court held, inter alia, that although the Fourth Amendment and Title III leave it to the discretion of law enforcement officials to decide how a search warrant or interception order is to be executed, the reasonableness of the execution is subject to judicial review. Normally such issues are litigated at an adversarial suppression hearing. This raises the question of whether a defendant is entitled to discover how entry was effected: unless a defendant knows what was done, it may be impossible for him to contest whether what was done was reasonable. On the other hand, disclosure might jeopardize subsequent use of the same methods in other cases.

At present, S. 1717 is completely silent on how much a defendant is entitled to learn about how entry was effected. Section 4 requires written notice to the issuing judge as to the time and method of entry. According to the section-by-section analysis that accompanied the bill's introduction, however, only a general statement as to method is required, e.g. "by a ruse, a subterfuge, a physical break-in, or some other method." The notice "need not detail every aspect of the mode of entry, such as the tools employed." It is not clear whether a defendant would be entitled to disclosure of such written notice at the suppression hearing; and, given the general nature of the written notice, such disclosure would hardly afford a defendant a true opportunity to contest the reasonableness of the specific method used.

A defendant should be allowed to discover the details of how entry was effected, subject, however, to two restrictions. The first restriction relates to standing. In general, a defendant has standing to contest the validity of an interception order or the manner of its execution only if his communications were intercepted or (if his communications were not intercepted) the surveillance occurred on his premises or over his telephone.¹ The mere fact that a defendant's oral communications were intercepted, however, may not necessarily give him standing to contest how the listening device was installed. Some courts have held that only defendants with a possessory or proprietary interest in the premises can contest the validity of surreptitious entry.²

The concern expressed by the F.B.I. and D.E.A. suggests a second restriction on discovery. In appropriate cases, the government should be permitted to submit an ex parte application to the trial (or hearing) judge, demonstrating that disclosure might compromise the safety of a cooperating

individual or would reveal highly sensitive and secret methods or equipment. If the judge is satisfied by the government's showing, he should conduct an in camera, ex parte proceeding on the reasonableness of how entry was effected, the record of which would be sealed. The defendant would be given an opportunity to present evidence on the issue, but would be denied discovery of the sealed record.

The concept of an ex parte suppression proceeding is unorthodox, but there are precedents. Two examples illustrate the point. When a grand jury witness refuses to answer questions on the ground that the questions are based on evidence derived from an invalid interception order, most federal courts have adopted a procedure whereby a judge conducts an ex parte examination of the interception application and order. The witness is denied access to the papers. If the court concludes that the papers are facially valid, the witness must answer the questions or be held in contempt. See Fishman, *Wiretapping & Eavesdropping* §§ 223-233 (Lawyer's Co-operative, 1978). The second example is provided by the Foreign Intelligence Surveillance Act of 1978. 50 U.S.C. § 1806(f) permits the Attorney General to invoke an in camera, ex parte suppression procedure if he attests in writing that disclosure of the details of the surveillance would jeopardize national security. See Fishman, *Wiretapping and Eavesdropping* § 374 (supp.).

Assuming the Committee agrees that such an ex parte proceeding should be allowed in appropriate cases, it must decide how to provide for such a proceeding. It might suffice if the Committee report expressly authorizes such a procedure. Alternatively, S. 1717 could be amended to include provision for such a procedure. Two additions to the bill may be worth considering in this regard.

A. Addition to 18 U.S.C. § 2518(8)(d)

18 U.S.C. § 2518(8)(d) governs post-interception notice generally. Its three subparagraphs require notice of the fact that an interception order or application was entered, the date that the order was granted or the application denied, and the fact that communications were or were not intercepted.

A fourth subparagraph could be added, to read:

- (4) if surreptitious entries were made onto a premises, the number of such entries.

This would assure that, even if no prosecutions result from the surveillance, notice of actual entry will be served on those whom the judge decides should receive it. If a non-defendant who receives such notice moves to discover the details, the judge has discretion to grant or deny such discovery.

B. Addition to 18 U.S.C. § 2518(9).

18 U.S.C. § 2518(9) requires the government to furnish a defendant with the interception order and application prior to trial, thereby alerting the defendant to bring a suppression motion. The language that now comprises § 2518(9) could be redesignated § 2518(9)(a). A new subdivision, designated 2518(9)(b), could be added, to read more or less as follows:

- (b) If surreptitious entry has been made onto a premises, the judge may in his discretion require the government to disclose the dates and times of such entries and details concerning how each entry was effected; provided, however, that if the government submits an ex parte showing that disclosure of dates, time or method would jeopardize the safety of any person or would compromise the future effectiveness of specific equipment or methods that were used to effect entry, the judge shall instead require the government to demonstrate at an ex parte proceeding that the methods used to effect entry were reasonable under the circumstances. All ex parte showings and proceedings conducted under this subsection shall be recorded and sealed.

It bears repeating that the ex parte procedure should be the exception, rather than the rule. In a case such as *Dalia*, where entry was effected by a break-in involving no secret equipment, the defendant should be entitled to disclosure. Only where the government demonstrates a valid need for secrecy would the ex parte procedure come into play.

Footnotes to question 3.

1. Only an "aggrieved person" may move to suppress intercepted communications or derivative evidence. 18 U.S.C. § 2518(10)(a). "Aggrieved person" is defined in 18 U.S.C. § 2510(11) as "a person who was a party to an intercepted wire or oral communication or a person against whom the interception was directed." The phrase "party to an intercepted wire or oral communication" is basically self-explanatory. The courts have interpreted the phrase "a person against whom the interception was directed" as affording standing to a non-intercepted communication only if the interceptions occurred over his telephone or on his premises. Alderman v. United States, 394 U.S. 165, 176-178 (1969); for similar holdings, see Fishman, Wiretapping and Eavesdropping § 165 at n. 17 (Lawyer's Co-operative, 1978).

2. United States v. Volpe, 430 F.Supp. 931, 945-46 (D. Conn. 1977). See also United States v. Scafidi, 564 F.2d 633, 638-639 (2d Cir. 1977). But see United States v. Costanza, 549 F.2d 1126, 1134 (8th Cir. 1977), holding that all defendants who had a right to be on the premises and had some reasonable expectation of privacy could contest the issue. Although these cases focus on the pre-*Dalia* issue of the constitutional and statutory validity of surreptitious entry generally, the same confusion is likely to emerge on the issue of who can contest the precise method of entry used. A similar division among the courts has developed as to who has standing to contest an alleged failure to minimize the interception of non-pertinent conversations. See Fishman, Wiretapping and Eavesdropping § 283 (1978).

Question 4. The bill speaks of covert entries by agents, and includes entries by ruse or subterfuge. Under your reading of the legislation, would it also apply to entries by agents who are given entry to a premises by a cooperating individual who has access to or by an undercover agent who is lawfully on the premises?

The bill defines "surreptitious entry" as including "both covert entry and entry effected by means of a ruse or subterfuge." In most cases, application of the definition will be fairly straightforward. The agents will want to enter the premises without letting anyone know what is being done, and such entries will require special authorization as spelled out in the bill. Still, where entry is achieved through the cooperation of a non-agent, or achieved by an undercover agent who is lawfully on the premises, interesting legal and practical problems arise.

A. Entry assisted by a cooperating individual.

I use the term "cooperating individual" to mean either a "good citizen" civilian or an informer who is paid on a per case basis or cooperates in the hopes of receiving leniency in cases pending against him.

In general, a person may consent to the search of a premises only if he or she shares a privacy interest in the premises. Thus, in United States v. Matlock, 415 U.S. 164 (1974), the woman with whom Matlock was living had the right to consent to the search of Matlock's house, and evidence seized during the search was admissible at trial. Entry obtained pursuant to such consent would not be surreptitious or covert in a true sense, even though the target of the surveillance would not know about it. Hence; such entry would not be within the provisions of the bill. See the section-by-section analysis.

On the other hand, if an aggrieved defendant learns at the suppression hearing that there had been an entry but that the procedures in S. 1717 were not followed, he may surmise that entry was achieved through the cooperation of someone with whom he shared the premises, a conclusion that could jeopardize the safety of such individuals. Hence, as a practical matter the government might choose to follow the S. 1717 procedures even though it would not be strictly necessary to do so, and then, at the suppression hearing, invoke the ex parte procedure suggested in my response to question 3.

B. Compelled Cooperation

In general, a landlord or custodian does not have the right to consent to the search of a tenant's premises, since it is the tenant's privacy, and not the landlord's, that is infringed. See Stoner v. California, 376 U.S. 483 (1964). However, 18 U.S.C. § 2511(2)(a)(ii) permits a landlord, custodian, communications common carrier, etc. to cooperate with law enforcement agents if (and only if) such cooperation is compelled by a court order issued pursuant to 18 U.S.C. § 2518(4). The court order must specify the type of cooperation required. Thus, a § 2518(4) order already satisfies all of the purposes of S. 1717: the judge has been informed of how entry is to be effected, and has issued an order authorizing the use of the method.

Nevertheless, situations might arise where the government might seek to utilize the proposed legislation, and the subsequent ex parte procedure discussed in my response to question 3, in order to prevent an aggrieved defendant from learning that the landlord or custodian cooperated with the agents.

C. Entry assisted by an undercover agent.

I assume the question contemplates a situation where, e.g., a DEA agent posing as a drug dealer is accepted into a social club where narcotics distribution is discussed and transacted. The agent might be able to plant the "bug" himself, or admit other agents for that purpose. Since the undercover agent's role is itself a ruse, it could be argued that S. 1717 procedures would have to be followed. This does not seem to be the purpose of the bill, however. The situation seems analagous to that of a cooperating individual (e.g. informer) who assists the agents. If S. 1717 does not apply to the informer, nor should it apply to the undercover agent. In both cases, the targets of the surveillance have assumed the risk that someone they trust is cooperating with the authorities. See United States v. Lewis, 385 U.S. 206 (1966); Hoffa v. United States, 385 U.S. 293 (1966); White v. United States, 401 U.S. 745 (1971); Smith v. Maryland, 99 S.Ct. 2577 (1979).

Question 5. In applying for the covert entry authority, would an agent have to demonstrate that the entry was the only means of effecting the interception?

The section-by-section analysis answers these questions to my satisfaction. All that need be shown is that it is impractical to obtain the interceptions without a surreptitious entry onto the targeted premises. With regard to interceptions of oral communications, the need for entry is virtually automatic. With regard to interception of wire communications, the special circumstances requiring entry should be spelled out.

Question 6. Does your reading of section 3 of the bill require the judge to find that a covert entry is the only or the best means of effecting the interception? What is the extent of the reviewing authority which the issuing judge has under this legislation?

Once a judge has signed an order authorizing the interception of oral communications, he really has little review authority concerning the need for surreptitious entry: the intercept order is likely to be a nullity without the authority to enter. In essence, the judge's role is to make sure the government has not neglected to include the required language in the application and order.

If the order authorizes interception of wire communication, the judge should insist that the application contain an explanation of the circumstances requiring entry.

Question 7. The Supreme Court in *Dalia* repeatedly stated that, while covert entries were implicit in the Title III intercept orders, such entries were subject to the reasonableness standard of the Fourth Amendment. Should the issuing judge make this determination before-the-fact or should it be left to the trial court judge?

- A. Can the issuing judge make such a determination without considering the actual circumstances of the entry itself?
- B. Under this standard, what type of entries would you consider to be "unreasonable?"

A. Reasonableness in general.

As the Supreme Court said in a slightly different context, whether the agents have acted reasonably will depend on the facts and circumstances in each case. Scott v. United States, 436 U.S. 128, 139-140 (1978) (interpreting the Title III minimization provision). Thus, even methods of effecting entry that upset or inconvenience innocent persons may be reasonable under some circumstances. For example, suppose federal agents use the guise of a bomb threat to evacuate an entire building in order to install a listening device in a particular apartment or office. It might be unreasonable to use this method if less intrusive means were available. And even if a bomb threat is the only practical way to install the device, it still might be unreasonable to stage a bomb threat at 2 a.m. in an apartment building if doing so at a more "civilized" hour would work just as well. Nevertheless, the bomb threat technique would not automatically be considered unreasonable (see section-by-section analysis).

In one circumstance, at least, an entry, by whatever means, would be unreasonable. If a judge concludes that the real purpose behind a re-entry was to conduct a physical search, it should be branded as unreasonable per se. While this might appear too obvious to be worth mentioning, I would suggest that the final Committee report mention it anyway, to safeguard against a subsequent Supreme Court decision that the agents' "subjective intent" is irrelevant if, "viewed objectively," the re-entry was nonetheless reasonable. (Compare the Supreme Court's misconstruction of the minimization provision in Scott v. United States, supra.)

B. Reasonableness depending upon crimes.

Should the reasonableness of a particular method of entry be measured only by the impracticality of less extreme methods, or should it also be assessed in light of the comparative seriousness of the crimes being investigated? If reasonableness is measured only against the impracticality of other means of gaining entry without regard to the particular designated offence being investigated, then the law, metaphorically speaking, may be placed in the position of endorsing use of a machine gun to swat a gnat. On the other hand, if the seriousness of the crime is a factor in assessing reasonableness, the judge may be required to make a value judgment as to how serious a particular crime is without the aid of objective standards to use as a guideline.

For example, suppose the only way that agents can enter a premises undetected is by using sleeping gas to immobilize a watchman. I would hold that this method is unreasonable if the target of the intercept order is a run-of-the-mill gambling operation: I would allow the gamblers to go unprosecuted, rather than endorse so distasteful a procedure. On the other hand, if this is the only means available to plant a bug needed to thwart a planned murder, kidnapping or airplane hijacking, I would have no qualms about holding the use of gas to be reasonable; indeed, I would commend the agents on their ingenuity. Suppose, though, that the murder already has been committed or the kidnap victim already has been ransomed, and the use of gas is the only practical method of planting a bug needed to identify and prosecute all those who had participated in the crime. Or suppose the crime being investigated is an extensive heroin distribution network. Would the use of gas be reasonable in either of these situations? What standards can a judge look to in deciding? I do not doubt that many judges would hold the use of gas to be abhorrent and never reasonable, while others probably would have fewer qualms than I about its use.

Concededly, these examples are somewhat far-fetched. They illustrate, however, just how ambiguous the word "reasonableness" may prove to be. If the committee determines that the crime being investigated should be a factor in assessing "reasonableness," the final committee report should say so explicitly.

C. Roles of issuing and trial judges

Section 4 of the bill requires only that the issuing judge be informed of the general method used to effect entry (e.g. ruse, break-in) unless he requests further information. (See section-by-section analysis.) Thus, the issuing judge may be in no position to assess the reasonableness of the method of entry. As a practical matter, therefore, the decision will normally be made by the trial judge.

On the other hand, if the issuing judge approves a particular method after being fully informed, his approval would be prima facie evidence that the chosen method was reasonable. In fact, such a finding could substitute for the ex parte, in camera proceeding suggested in my response to question three. Hence, it might be in the government's best interest to provide the issuing judge with more information than he would otherwise request. An obvious parallel exists with regard to minimization: several courts have held that where the issuing judge has been kept informed of the manner in which interceptions were conducted, that judge's approval constitutes a prima facie finding that the agents' conduct was reasonable. See Fishman, Wiretapping and Eavesdropping § 173 (1978).

Question 8. Under the provisions of this legislation, if the issuing judge determines that a subsequent re-entry was unreasonable or refuses to authorize such re-entry, what recourse would the court or the government have in these situations?

If the government informs the issuing judge that re-entry will be necessary and the judge disagrees, section 4 (p. 4, lines 8-19, proposed 18 U.S.C. § 2518(4)(g)(iii)) implicitly empowers the judge to forbid the government to make the re-entry. Requiring that the judge be notified is meaningless unless the judge is authorized to prevent re-entry. Similarly, if the government notifies the judge after re-entry and the judge concludes that the re-entry was unnecessary or was effected in an unreasonable manner, the provision would appear to give the judge implicit authority to terminate the intercept order. Without such authority, the judge would be little more than a clerk.

In either situation, the judge in essence is entering an ex parte suppression order prior to any arrests or indictments. This is highly unusual, but not without precedent. Congress enacted the progress report provision of Title III (18 U.S.C. § 2518(6)) in part to provide a mechanism whereby the issuing judge could terminate the surveillance if he becomes convinced that further interceptions are unnecessary. S. Rep. # 1097, 90th Cong., 2d Sess. 104, reprinted in (1968) U.S. Code, Cong. Admin. News 2193. Section 4 of S. 1717 gives the judge similar authority in the surreptitious entry context.

I know of no cases in which an issuing judge exercised the power to terminate surveillance granted in 18 U.S.C. § 2518(6); certainly no such cases have been reported. I would anticipate that the termination power implicit in section 4 of S. 1717 will be used with the same approximate frequency. Should a judge order the surveillance terminated, the government presumably would be able to bring an expedited appeal.

Question 9. We have been told by a number of investigative agencies that it is difficult, if not impossible, to determine ahead of time the exact method and time of entry. Does this legislation provide adequate flexibility so that both the time and method could be changed if circumstances so dictated?

Section 4 authorizes entry without prior notification to the judge if the agents are presented with a fleeting opportunity that must be exploited immediately or not at all. Implicitly, the agents could also exploit such an opportunity even if the government attorney has already notified the judge of a different proposed time and method, so long as the judge is given written notice of what has been done within forty-eight hours. See section-by-section analysis. Thus, the legislation provides the necessary flexibility.

Question 10. This legislation also provides for a new emergency exception to the provisions of Title III for situations involving immediate danger of death or serious bodily injury. Do you have any comments about the need for this provision?

- A. *In determining whether such danger is "immediate," how broadly or narrowly should this provision be read?*
- B. *What factors should Federal agents take into account to determine the immediacy of the danger? For instance, in a hostage situation, how should an agent determine whether such a danger exists and whether it is immediate?*

The best way I can address this question is to set out four hypothetical situations. In each, assume that the grounds for an interception order exist, i.e. there is probable cause to believe that a crime is being or is about to be committed, there is probable cause to believe that the interception of communications occurring in a specific premises or over a specific telephone will reveal evidence of a crime, and normal investigative procedures have not or likely would not provide the information necessary to thwart the crime and apprehend the criminals. Assume further that the crime is one that threatens death or serious physical injury to one or more persons.

A. There is probable cause to believe that the crime will be attempted before an interception order can be obtained. Even under the narrowest reading of the provision, emergency surveillance would be justified in such a situation.

B. The authorities are uncertain when the crime is to be attempted: perhaps before an interception order can be obtained, perhaps not for several days or weeks. In my opinion, emergency surveillance would be justified in this situation, since there is a realistic possibility that death or serious injury might be prevented if surveillance is conducted before an order can be obtained.

C. The crime is to be attempted at a specified date several weeks hence (e.g. at a political convention that will occur in one month's time). Although the danger itself is not imminent, there is a possibility that once the participants in the plot have finalized their plans, they will go underground separately and will not meet again, but will carry out their individual roles according to the plan. Hence, surveillance before an order can be obtained might present the best or even the only opportunity to foil the plot by revealing the identity of the intended victim, or the details of the plot.

This situation presents a rather broad reading of "immediate," but I think pre-interception order surveillance nevertheless should be permitted: without immediate surveillance, the danger of death or serious physical injury to the intended victim or victims increases substantially. The situation is analogous to one where police have probable cause to believe that evidence of crime currently exists but that the evidence is likely to be moved or destroyed before a search warrant can be obtained. Most courts have agreed that an immediate search and seizure would be justified under such exigent circumstances.¹

Concededly, to read the provision this broadly increases the possibility for abuse. Nevertheless, the likelihood of unjustified surveillance is slight. The Attorney General's personal approval is required before such surveillance is authorized. 18 U.S.C. § 2518(7). If a judge subsequently concludes that surveillance was unjustified, the fruits of the surveillance will be suppressed and all those who participated in the surveillance will be susceptible to a civil suit for damages pursuant to 18 U.S.C. § 2520. These existing provisions in Title III should substantially safeguard against unnecessary surveillance. On the other hand, permitting surveillance under the circumstances presented in the third hypothetical situation could save lives. Since the risk of abuse is small and the potential good that could be accomplished is great, pre-interception order surveillance should be permitted under such circumstances.

D. Hostages have been taken or a victim has been kidnapped. Here, no further showing of "immediacy" should be required, since the situation is inherently dangerous to the life and health of the victims.

Note to question 10.

1. See, e.g. United States v. McKinney, 477 F.2d 1184 (D.C. Cir. 1973); Wayne v. United States, 318 F.2d 205 (D.C. Cir. 1963) (Burger, J.). Although the Supreme Court has not expressly so held, dictum in several cases appears to recognize the exigent circumstances exception. Schmerbef v. California, 384 U.S. 757 (1966); Chambers v. Maroney, 399 U.S. 42 (1970); Vale v. Louisiana, 399 U.S. 30 (1970); Williams v. United States, 401 U.S. 646 (1971); Mincey v. Arizona, 437 U.S. 385 (1978). See generally 2 LaFave, Search and Seizure 432 - 466 (West, 1978).

Question 11. Other than hostage situations, can you give any other examples of where this exception might be necessary?

Emergency surveillance could prove helpful in a variety of situations: to thwart a murder or kidnap plot, a bombing, an incitement to riot, an airplane hijacking; in fact, any situation in which violence is threatened and there is an immediate need for the surveillance.

Question 12. Are you aware of any instances in which the current exceptions to the provisions of Title III regarding organized crime and national security have been invoked?

The National Wiretap Commission Report (1976) at 111 - 113 discusses three instances, one federal and two state, in which emergency surveillance was conducted. Reported court decisions are rare. See State v. Nabozny, 375 N.E.2d 784 (1978) (Ohio) and Shingleton v. State, 39 Md. App. 527, 387 A.2d 1134, 1139 (1978), neither of which is particularly illuminating.



United States Department of Justice

ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
WASHINGTON, D.C. 20530

31 MAR 1980

Honorable Patrick J. Leahy
Subcommittee on Criminal Justice
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Senator Leahy:

Attached are our responses to the questions you posed concerning the provisions of S. 1717 in your letter of March 6, 1980.

I want to thank you for the opportunity to testify before the Subcommittee on this bill which would serve the distinct but equally important interests of privacy and the preservation of human life. If I can provide any other materials that would be of assistance to the Subcommittee in its consideration of this bill, please contact me.

Sincerely,

Philip B. Heymann
Assistant Attorney General
Criminal Division

COVERT ENTRIES

1. What are some of the advantages of a microphone eavesdrop over a wiretap?

As Mr. Colwell noted in his testimony, from a technical standpoint, microphone eavesdrops are more problematic than wiretaps. The advantage of a microphone eavesdrop is simply that it permits the interception of face-to-face conversations. Thus the use of microphones can be a valuable investigative tool, for example, when it is known that a meeting is to take place where the planning or execution of an illegal transaction is to occur. A wiretap, on the other hand, is used to intercept telephone conversations.

Although under certain circumstances, the use of a microphone eavesdrop is clearly advantageous, as a general rule, these eavesdrops are used with less frequency than wiretaps. First, installation of a microphone ordinarily requires a covert entry, yet accomplishing this entry is not always possible. Second, because a microphone generally represents a more serious intrusion than a wiretap, the sufficiency of an application for the interception of oral communications is scrutinized with extreme care. Finally, as a general matter, it is more difficult to obtain "probable cause" for a microphone eavesdrop.

2. Would you briefly describe the operational considerations and potential difficulties with covert entries?
 - A. What types of preparation are done prior to such entries?
 - B. How much information about the premises can be obtained prior to your determination regarding the time and method of entry?

Two primary considerations in using covert entry are the protection of the agents who make the entry and the need to assure that the entry and its purpose are not discovered prior to the termination of the interception. In preparation for a covert entry, physical surveillance and other fundamental investigative approaches are used to determine the best time and method for an attempted entry. Sometimes extensive information about the premises is available through informants who have access to the location, or through a pretense overt entry. However, in many cases very little specific information about the premises can be obtained prior to the attempted entry.

3. Is it possible to determine in advance of the entry the exact time and method of that entry? If not, why not?

The only situation wherein we might determine, in advance, the exact time and method of entry is where a cooperating individual arranges to give us access to that location. This cooperating individual would be someone who has control over

or proper access to the location where the entry is to be made. A concern that arises in such a situation is that the specification, in advance, of the exact time and method of entry, if made available to the target would serve to signal the target that an informant has access to the premises. Of course, even where we have such cooperation, unforeseen changes in circumstances may arise, as they frequently do in other instances, which necessitate changing the time and method of entry.

4. Under your reading of this legislation, is there an adequate amount of flexibility to allow for last-minute changes in the time or method?

By providing that the issuing judge may be notified of a change in time or method of entry within 48 hours of the entry when prior notice is not practicable, sufficient flexibility is provided.

5. Since the Supreme Court in *Dalia* has held that a covert entry provision is not a required part of the Title III order, what benefits do you see flowing from this legislation?

The Court's holding was based on two points. First, the Court reasoned that since the interception of oral communications almost always will require that a surreptitious entry be made to install a microphone -- and indeed this is the case -- it was reasonable to assume that judges would be aware in approving an interception of oral communications that a surreptitious entry was anticipated. However, since relatively few such orders are granted each year, a judge called upon to authorize the interception of oral communications may not be fully aware of the methods that must be utilized to effect the interception. This bill will assure that the issuing judge recognizes the methods of executing the order that will be employed. Second, the Court noted that in the area of searches and seizures generally, the judge issuing the warrant does not consider and rule on the reasonableness of the proposed mode of executing the warrant. However, the execution of a search warrant is overt, while the installation of a bug in electronic surveillance is covert. Thus in a Title III interception, there is no contemporaneous notice to the occupants of the premises that an intrusion into the privacy of their homes or offices has taken place. Hence surreptitious entries can be particularly intrusive, and the persons whose privacy has been invaded certainly are not in a position to observe the execution of the order and bring the manner in which it is executed to the attention of the court as effectively as in the case of a search and seizure. Thus the participation of an informed, impartial judge seems appropriate in the case of surreptitious entries made to execute Title III orders. Furthermore, we have found that our present policy regarding

surreptitious entries, which is much like the requirements set out in S. 1717, is not burdensome.

6. The Supreme Court noted with approval the Department of Justice policy to include covert entry provisions in Title III orders and suggested that it was the "preferable approach." How long has the Department had this policy? To what extent does the current policy of the Department differ from the provisions of this legislation?

The Department policy regarding covert entry is the area of electronic surveillance has been in effect formally since November, 1978.

Our present policy requires that the application for a Title III order state whether surreptitious entry is to be used, and that the order sought specifically authorize the use of such entry and identify the agency authorized to make the entry. S. 1717 contains the same core requirements. Of course our policy does not set forth the standard by which the issuing judge is to determine whether surreptitious entry is to be approved. This legislation provides just such a standard: in order to approve the covert entry, the issuing judge must find that such entry "reasonably appears to be required to effect the interception because other means of effecting the interception than surreptitious entry reasonably appear to be unlikely to succeed, too dangerous, or impracticable." In addition, our policy does not require that prior written notice be given to the issuing judge of the specific time and method of the proposed entry. This information may be provided, however, in the periodic reports which are submitted to the judge to apprise him of the progress of the interception. Similarly, our policy does not require prior written notice of subsequent re-entries, although such a practice is frequently followed. Thus while the approaches of our policy and the provisions of S. 1717 differ somewhat, on the whole they are substantially similar.

7. In some instances, it is necessary for agents who are installing a Title III intercept device to re-enter the premises. Do you know the number of such situations in the past where such re-entry was necessary and why it was necessary?

A. Does this legislation adequately provide for re-entry situations?

It would be almost impossible to determine the number of situations wherein our agents were required to make re-entries into a target location. However, in recent years (in some districts) our agents have notified the court when re-entry was necessary, and so information is retrievable in those cases. Discussions with personnel who have been involved in numerous installations revealed that re-entry is necessary

in almost every situation involving the installation of a microphone, e.g., for the purpose of repair, relocation, re-activation, or removal. It is preferable to remove such devices through a covert approach in order not to reveal immediately the location and configuration of our listening devices.

The legislation adequately provides for re-entry situations. As the section - by - section analysis points out, a new application and order are not necessary for each re-entry. However, there is a provision for written notice to the issuing judge of subsequent re-entries which is sufficiently flexible in that it permits notice within 48 hours when prior notice is not practicable. This flexibility takes into account the fact that situations may arise in which it is necessary to quickly re-enter to make a repair or adjustment.

8. The bill speaks of covert entries by agents and includes entries effected through ruse of subterfuge. Under your reading of this legislation, would these provisions also apply to entries by agents who are given entry to a premises by a cooperating individual who has access to or by an undercover agent who is lawfully on the premises?

The provisions of the bill would not apply to such entries when we were given access to the premises by a person with authority to do so. These situations are analogous to those in which there is valid consent given to conduct a search of a dwelling or office, and established law regarding consensual searches can provide guidance in this area. However, if there were a question whether the person through whom we have access is in fact in a position to consent to such an entry, our agents should seek specific authorization as provided in the bill.

9. Does your reading of section 3 of the bill require the judge to find that a covert entry is the only or the best means of effecting the interception?

- A. What is the extent of the authority which the issuing judge has under this legislation?

This is a very important issue in our view. First, the issuing judge need only find that "surreptitious entry reasonably appears to be required to effect the interception because means of effecting the interception other than surreptitious entry reasonably appear, if tried, to be unlikely to succeed, too dangerous, or impracticable," not that it is the only means of effecting the interception. Indeed as the section-by-section analysis points out, when the interception of oral communications is authorized, generally the only

feasible means of effecting the interception is through the surreptitious installation of a microphone. Thus in the case of oral communications no extraordinary demonstration of the need to enter surreptitiously is mandated by the bill. We urge that such clarifying language be adopted for inclusion in the legislative history of the bill. The primary purpose of the bill is to assure that issuing judges are aware that such entry will be used, not to effectively preclude the interception of oral communications by imposing a requirement of extraordinary necessity to justify the resort to surreptitious entry. However, if the judge should find that the required showing has not been made, he may not authorize the entry, and without specific authorization, the use of surreptitious entry is prohibited.

10. You have told us that notification of the time and method of entry by the government attorney would jeopardize subsequent use of these methods in other investigations. Could you explain this problem in light of the fact that the time and method will be brought to light during the course of pre-trial motions?

- A. What changes should be made in the legislation to protect entry methods?

Our concerns revolve around the degree of detail and specificity regarding our investigative techniques that might be required in the proposed notice of method of entry provision. If such information were made available routinely to others than the court, it might severely undercut the continued effectiveness of our investigative techniques.

However, as you point out, the reasonableness of all aspects of the interception may be subject to pretrial motions, even absent the notice provisions of the bill. Thus the method of entry could be revealed in these motions. However, the operation of these notice provisions could result in disclosure in many instances where the method of entry would not be the subject of a pre-trial motion. First, because of the strength of evidence obtained by electronic surveillance, many cases may result in guilty pleas, so there will be no pre-trial hearings. Second, the defendant may have no privacy interests in the premises entered, and thus may not have standing to raise the issue of the reasonableness of the entry at a pre-trial hearing. Third, the existing notice provisions of 18 U.S.C. 2518(8)(b) require notice to all persons who have been parties to intercepted communications of the fact of the interception and permits their inspection of the papers filed with the court relating to the interception. All those persons will not necessarily be defendants, of course, and thus would not be bringing pre-trial motions in which the mode of entry would be at issue. In addition, where such persons have no privacy interest in the premises which were entered, they would not be in a position to challenge the method of entry.

To assure that the continued effectiveness of our investigative techniques is not compromised, we urge, at a minimum, that the bill itself incorporate the language that appeared in the section-by-section analysis which accompanied the bill at its introduction which provided that a statement indicating whether the entry was to be accomplished by a physical break-in or a ruse would be sufficient to meet the requirement of the notice of the method of entry. Of course, even absent any statutory requirement concerning disclosure of the method of entry, the issuing judge would have the authority to require a thorough explanation of the proposed method of entry on a case-by-case basis.

11. The Supreme Court in *Dalia* repeatedly stated that, while covert entries were implicitly authorized in Title III intercept orders, such entries were subject to the reasonableness standard of the Fourth Amendment. Should the issuing judge make this determination before-the-fact, or should it be left to the trial judge? Why?

- A. Under this standard, what type of entries would you consider to be "unreasonable"?

This bill would require the issuing judge to make a before the fact reasonableness determination regarding the use of surreptitious entry. Because covert entry presents unique privacy considerations, we believe that it is appropriate that the issuing judge be alerted to the fact that such entry is contemplated. We could note, however, that in most cases involving interception of oral communications surreptitious entry would be reasonable because it is the only available method of accomplishing such interception.

Although the issuing judge would be making an initial reasonableness determination with regard to the use of surreptitious entry, the reasonableness of the entry would be subject to subsequent review by the trial judge, for example, in the context of a motion to suppress. At this stage the reasonableness of the particular mode of entry could be examined.

The only examples of "unreasonable" entries we can pose are hypothetical, for we are unaware of any entries conducted by our agents in such a way as to be considered unreasonable. Examples of "unreasonable" searches might be a bomb scare ruse that required evacuation of a neighboring hospital, an entry and installation that required substantial property damage, or breaking and entering to install a wiretap where exterior lines could have been easily tapped.

12. Under the provisions of this legislation, if the issuing judge determines that a subsequent re-entry was unreasonable or refuses to authorize a re-entry, what recourse would the court or the government have in these situations?

If such determinations result in suppression of evidence or are in effect a denial of the application, the government may seek an appeal as currently provided under 18 U.S.C. 2518(10)(b). However, our first step would be to try to accommodate the concerns of the judge, either by producing further evidence of the necessity of the entry, or by proposing an alternative method entry.

13. Have there been instances in the past where covert entries could not be made to install Title III intercept devices? Why was this?

Such situations have arisen because the security devices used at a location were either impenetrable or an attempt was considered either too dangerous for our agents or too likely to result in discovery by the targets of the investigation.

LIFE-ENDANGERING EXCEPTION

14. Title III currently allows for two types of emergency situations -- those dealing with conspiratorial activities which threaten the national security, and those which are characteristic of organized crime. How often have these exceptions been invoked and under what circumstances?

- A. To your knowledge, have the Federal courts ever interpreted the scope or applicability of these exceptions?

Section 2518(7) has been invoked only for conspiratorial activities which are characteristic of organized crime. Since 1968 our best estimate is that the provision has been invoked between 10 and 15 times. The provision has been invoked only in situations involving immediate danger to human life, (kidnapping and hostage taking), except, we believe, in one instance.

While the Federal courts have interpreted the provision when the Department of Justice applied for a court order within the 48 hours, we know of no reported Federal case which interprets the provisions. For jurisdictions other than Federal jurisdictions that interpret the provision or parallel local provision see Khaalis v. United States, 408 A.2d 313 (D.C. Ct. App. 1979); Shingleton v. Maryland, 387 A.2d 1134 (Md. Ct. Sp. App. 1978); State v. Nabozny, 54 Ohio St. 2d 195 (1978), vacated in part on other grounds, 439 U.S. 811 (1978).

15. Section 5 of the bill provides for a new emergency exception to the provisions of Title III for situations involving immediate danger of death or serious bodily injury.
 - A. How have these situations been handled in the past years?
 - B. How many of these situations have arisen since Title III went into effect?
 - C. What is the current legal basis for emergency interceptions in these cases?

A request for approval of an emergency interception is to be reviewed by the Attorney General. In his absence, a designated Assistant Attorney General may exercise the power conferred by 18 U.S.C. 2518(7). If available, it is the Assistant Attorney General for the Criminal Division, who would exercise this authority in the absence of the Attorney General. The request must not only set forth the bases for invoking the emergency interception provision, but also the grounds under which a Title III judicial order would be obtained if time permitted.

As stated above, our best estimate is that 10-15 emergency authorizations have been granted. In addition there have been requests for authorization which have been denied, and instances in which a request was made but our negotiators were able to obtain release of victims or hostages before authorization was forthcoming.

The legal basis for these emergency interceptions has been the provision concerning activities characteristic of organized crime. This phrase is not defined in the statute, and our need to preserve human life has in some instances demanded a somewhat expansive reading of this provision. It is for this reason that we seek the clarification of authority in S. 1717. In addition to the existing basis for emergency interceptions under 18 U.S.C. 2518(7), other legal bases have been advanced as the source of authority in these situations. First when oral communications take place before victims or hostages there is a strong argument that there is no expectation of privacy. Second, the Department has argued that a trespassing hostage taker has no standing to contest the interception of his or her communications. (See *Khaalis v. United States*, 408 A.2d 313 (D.C. Ct. App. 1979).) Third, the argument has been advanced that there is implicit in the statute itself an exception permitting emergency interceptions in truly exigent circumstances involving a threat to human life.

16. How broadly or narrowly should the term "immediate" danger be read?
 - A. What factors should Federal agents take into account to determine the immediacy of the danger? For instance in a hostage situation, how should an agency determine whether such a danger exists and whether it is immediate?

We are aware that too broad a reading of the term "immediate" danger could open the door to abuse. On the other hand, our ability to save life should not hinge on meeting an overly narrow standard, or the very purpose of the amendment would be lost. Factors that might be considered would be a hostage taker's access to weapons, express or implied threats of violence, knowledge of a past history of committing violent crimes, the lack of opportunity for direct physical intervention by law enforcement officers, and the condition of the victim.

It has been our experience in past cases that there often will be little doubt about the immediacy of the danger to human life, for hostage takers and kidnappers will make clear their willingness to kill or injure their victims in order to force

action on their demands. Furthermore, our agents are specially trained, indeed agents on the scene may be specialists in hostage negotiations, to assess the immediacy of the danger.

In general, we would interpret "immediate" danger to human life to mean any situation in which an intent or willingness to injure or kill is present, the means for committing such an act exist, and the time within which the anticipated or threatened act of violence may occur is short. Thus we believe that in the vast majority of hostage situations, where a person is being held captive by force, an immediate threat to life will exist.

17. Other than hostage situations, what other types of crimes or life-endangering situations would trigger this new exception?

Life endangering situations over which the FBI has jurisdiction include Assaulting the President, Congressional Assassination, Extortion, Assaulting a Federal Officer, and Kidnapping, to cite just a few examples. In any of these matters or during the course of FBI investigation of organized crime it is possible that information could be received indicating a potential violation of these statutes and immediate danger to an individual. Of course not all potential violations of these statutes would constitute immediate danger to human life.

18. Under the current policy of the Department of Justice, who would be the "investigative or law enforcement officer specially designated by the Attorney General" who would determine the existence of an emergency situation and approve the use of this exception?

The specially designated official would ordinarily be the head of the federal agency requesting the emergency authorization, such as the Director of the FBI. The Attorney General, after receiving such a request may designate the Director to proceed as required by the statute or he may determine that the emergency procedure is not appropriate and direct the applicant to apply for a court order. If the Attorney General is not available it is an Assistant Attorney General who will be the "specially designated" officer who will determine the existence of the emergency, make the probable cause determination, and, if appropriate, approve the request.



United States Department of Justice

ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
WASHINGTON, D.C. 20530

31 MAR 1980

Honorable Joseph R. Biden
Subcommittee on Criminal Justice
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

This letter is in response to your request for my comments on S. 1815, a bill which would amend Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to require specific judicial authorization for any covert entry made to install or remove an electronic surveillance device. The purpose of S. 1815 is the same as that of the surreptitious entry provisions of S. 1717 which we fully supported in our testimony before the Subcommittee on March 5, and that is to require notice to the issuing judge of the anticipated use of covert entry, to set forth a standard by which the issuing judge is to assess the reasonableness of the use of such entry, and to require that his authorization of the use of surreptitious entry be set out in the court's order authorizing the interception. Thus, while S. 1815 is less detailed than S. 1717, it is designed to advance the same sort of procedural principles and in this respect we fully support its intent.

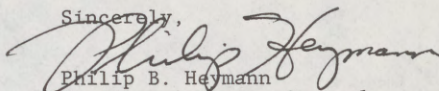
There are, however, three problems presented by S. 1815 upon which I would like to comment. First, the term "covert entry" is not defined. Thus, it is not clear whether this term would encompass, as does the term "surreptitious entry" in S. 1717, both entries accomplished by a ruse and entries which would constitute a physical break-in. Senator Nelson, in his remarks which accompanied the bill at its introduction, referred only to entries which would consist of a breaking and entering, so it may be that entries by ruse are not intended to be included. We believe it is appropriate that these procedural requirements apply to both covert physical entries and entries by ruse or subterfuge.

Second, the bill characterizes covert entries as "illegal" entries which are to be distinguished from "legal" entries, and requires as a prerequisite to obtaining authorization for covert entry a demonstration that the use of a "legal" entry to install the interception device would be impracticable. A non-trespassory entry by our agents, i.e. one in which they gave notice of the entry and its purpose, would never be a feasible means of effecting the installation of an interception device. Such notice would defeat the purpose of the interception itself by alerting the targets of the interception. Furthermore, it is inappropriate to characterize covert entries as "illegal" since the Supreme Court in United States v. Dalia, 441 U.S. 238 (1979) held that such entries in the context of effecting an electronic surveillance were not, per se, violative of either Title III or the Fourth Amendment.

Finally, S. 1815 speaks only of the authorization of covert entries for the purpose of installing or removing an interception device. The experience of our agents has been that re-entries for the purpose of maintenance, repair, and adjustment of these devices are frequently necessary. Thus, in our view, inclusion of re-entry for these purposes under the provisions of the bill is appropriate.

While we are concerned about the three aspects of the bill discussed above, the Department supports the purpose of S. 1815. Like the more detailed provisions of S. 1717, the procedural requirements prescribed by S. 1815 would assure that covert entry is employed to effect Title III surveillance only when authorized by an informed judicial officer. It is our judgment that such procedures, which indeed are currently reflected in Department of Justice policy, are appropriate in view of the privacy concerns which arise from covert entries.

Sincerely,



Philip B. Heymann
Assistant Attorney General
Criminal Division.

ADMINISTRATIVE OFFICE OF THE
UNITED STATES COURTS

WASHINGTON, D.C. 20544

WILLIAM E. FOLEY
DIRECTORJOSEPH F. SPANIOL, JR.
DEPUTY DIRECTORJAMES A. MCCAFFERTY
CHIEF
STATISTICAL ANALYSIS AND
REPORTS DIVISION
FTS 633-6094
202-633-6094

August 31, 1979

Honorable Edward M. Kennedy
United States Senate
2241 Dirksen Senate Office Building
Washington, D. C. 20510

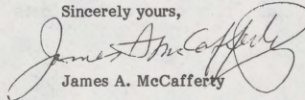
Dear Senator Kennedy:

In response to your request of August 28, 1979, we have prepared tables on the number of state and federal intercepts installed, by location and type, during calendar years 1968 through 1978. The tables are as follows:

1. Table 1, State and Federal Phone Wire Intercepts Installed, by Location, for the Years 1968 through 1978;
2. Table 2, State and Federal Microphone-Eavesdrop Intercepts Installed, by Location, for the Years 1968 through 1978;
3. Table 3, State and Federal Phone Wire/Microphone Eavesdrop Intercepts Installed, by Location, for the Years 1968 through 1978; and
4. Table 4, State and Federal Intercepts Installed Using Other Types of Surveillance, by Location, for the Years 1968 through 1978.

In addition we are enclosing a copy of the report instructions, the docket set, and the Wiretap Report for calendar year 1978.

Sincerely yours,


James A. McCafferty

Enclosures

Table 1
State and Federal Phone Wire
Intercepts Installed, by Location,
for the Years 1968 through 1978¹

Jurisdiction and Year	Total Installed	Location					
		Single Family Dwelling	Apart- ment	Multi- dwelling	Business	Combina- tion ²	Other
Total Federal and State	6,096	2,537	1,600	397	1,012	320	230
Total Federal	1,160	424	308	48	163	179	38
1968	-	-	-	-	-	-	-
1969	27	10	7	3	7	-	-
1970	171	49	56	4	33	22	7
1971	270	115	78	11	30	27	9
1972	187	64	57	10	14	31	11
1973	105	41	29	6	13	15	1
1974	97	36	20	5	14	20	2
1975	83	26	23	4	11	18	1
1976	109	44	26	1	14	20	4
1977	57	16	8	3	9	18	3
1978	54	23	4	1	18	8	-
Total State	4,936	2,113	1,292	349	849	141	192
1968	147	57	44	6	40	-	-
1969	222	110	55	9	45	3	-
1970	367	144	91	34	70	8	20
1971	483	219	124	30	90	9	11
1972	592	276	149	43	86	10	28
1973	626	243	186	48	102	11	36
1974	536	204	123	51	111	22	25
1975	537	224	154	28	92	22	17
1976	472	200	125	49	67	12	19
1977	498	220	136	25	70	26	21
1978	456	216	105	26	76	18	15

¹1968 data covers the period June 20 - December 31, 1968. All other data is for the entire calendar year.

²Combination refers to the number of authorized interceptions where more than one location was reported.

Prepared by the Administrative Office of the U.S. Courts, Statistical Analysis and Reports Division,
Washington, D.C. 20544.

Table 2
State and Federal Microphone-Eavesdrop
Intercepts Installed, by Location,
for the Years 1968 through 1978¹

Jurisdiction and Year	Total Installed	Location					Other
		Single Family Dwelling	Apart- ment	Multi- dwelling	Business	Combina- tion ²	
Total Federal and State	282	19	38	6	137	5	77
Total Federal	79	6	11	3	43	2	14
1968	-	-	-	-	-	-	-
1969	1	-	-	-	1	-	-
1970	3	-	1	-	2	-	-
1971	5	-	1	-	2	-	2
1972	5	-	2	-	2	-	1
1973	12	2	1	-	5	-	4
1974	10	1	-	1	7	-	1
1975	11	1	3	-	5	1	1
1976	10	-	1	-	5	1	3
1977	9	2	1	1	4	-	1
1978	13	-	1	1	10	-	1
Total State	203	13	27	3	94	3	63
1968	-	-	-	-	-	-	-
1969	14	-	1	-	8	-	5
1970	18	-	4	1	6	-	7
1971	12	1	1	-	4	-	6
1972	24	1	2	-	7	1	13
1973	36	7	6	-	14	-	9
1974	26	-	6	1	14	1	4
1975	26	1	5	-	15	-	5
1976	16	1	-	-	9	1	5
1977	17	2	2	1	5	-	7
1978	14	-	-	-	12	-	2

¹1968 data covers the period June 20 - December 31, 1968. All other data is for the entire calendar year.

²Combination refers to the number of authorized interceptions where more than one location was reported.

Prepared by the Administrative Office of the U.S. Courts, Statistical Analysis and Reports Division,
Washington, D. C. 20544.

Table 3
State and Federal Phone Wire/Microphone
Eavesdrop Intercepts Installed, by Location,
for the Years 1968 through 1978¹

Jurisdiction and Year	Total Installed	Location					
		Single Family Dwelling	Apart- ment	Multi- dwelling	Business	Combi- nation ²	Other
Total Federal and State	203	22	34	5	80	42	20
Total Federal	103	8	8	1	47	36	3
1968	-	-	-	-	-	-	-
1969	2	-	-	-	-	2	-
1970	5	1	1	-	3	-	-
1971	6	-	1	-	2	3	-
1972	13	1	1	-	4	5	2
1973	13	2	2	-	5	4	-
1974	13	-	1	-	7	5	-
1975	12	-	-	1	9	2	-
1976	15	-	1	-	7	6	1
1977	11	1	1	-	5	4	-
1978	13	3	-	-	5	5	-
Total State	100	14	26	4	33	6	17
1968	-	-	-	-	-	-	-
1969	4	1	2	-	1	-	-
1970	18	3	9	-	3	-	3
1971	8	1	2	1	1	-	3
1972	15	2	2	2	4	1	4
1973	19	2	5	-	9	-	3
1974	5	-	1	-	4	-	-
1975	7	-	3	-	2	2	-
1976	10	2	1	-	4	1	2
1977	7	2	1	1	2	1	-
1978	7	1	-	-	3	1	2

¹1968 data covers the period June 20 - December 31, 1968. All other data is for the entire calendar year.

²Combination refers to the number of authorized interceptions where more than one location was reported.

Prepared by the Administrative Office of the U.S. Courts, Statistical Analysis and Reports Division,
Washington, D.C. 20544.

Table 4
State and Federal Intercepts Installed Using
Other Types of Surveillance, by Location,
for the Years 1968 through 1978¹

Jurisdiction and Year	Total Installed	Location					Other
		Single Family Dwelling	Apart- ment	Multi- dwelling	Business	Combi- nation ²	
Total Federal and State	29	8	5	-	6	2	8
Total Federal	3	1	-	-	-	1	1
1968	-	-	-	-	-	-	-
1969	-	-	-	-	-	-	-
1970	-	-	-	-	-	-	-
1971	-	-	-	-	-	-	-
1972	-	-	-	-	-	-	-
1973	-	-	-	-	-	-	-
1974	-	-	-	-	-	-	-
1975	-	-	-	-	-	-	-
1976	2	-	-	-	-	1	1
1977	-	-	-	-	-	-	-
1978	1	1	-	-	-	-	-
Total State	26	7	5	-	6	1	7
1968	-	-	-	-	-	-	-
1969	-	-	-	-	-	-	-
1970	-	-	-	-	-	-	-
1971	8	3	-	-	2	1	2
1972	5	-	2	-	1	-	2
1973	1	1	-	-	-	-	-
1974	7	2	3	-	1	-	1
1975	-	-	-	-	-	-	-
1976	1	-	-	-	1	-	-
1977	2	1	-	-	1	-	-
1978	2	-	-	-	-	-	2

¹1968 data covers the period June 20 - December 31, 1968. All other data is for the entire calendar year.

²Combination refers to the number of authorized interceptions where more than one location was reported.

Prepared by the Administrative Office of the U.S. Courts, Statistical Analysis and Reports Division,
Washington, D.C. 20544.