98th Congress
2d Session

SENATE

REPORT
98–660

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978: THE FIRST FIVE YEARS

REPORT

OF THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

egislative day, SEPTEMBER 24), 1984.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1984

CONTENTS

98TH CONGRESS } SENATE { REPORT
2d Session } { 98–660

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978: THE FIRST FIVE YEARS

OCTOBER 5 (legislative day, SEPTEMBER 24), 1984.—Ordered to be printed

Mr. GOLDWATER, from the Select Committee on Intelligence, submitted the following

REPORT

The Foreign Intelligence Surveillance Act of 1978: The First Five Years

I. INTRODUCTION

The Foreign Intelligence Surveillance Act of 1978 (FISA) established comprehensive legal standards and procedures for the use of electronic surveillance to collect foreign intelligence and counterintelligence within the United States. The Act provided the first legislative authorization for wiretapping and other forms of electronic surveillance for intelligence purposes against foreign powers and foreign agents in this country. It created the Foreign Intelligence Surveillance Court, composed of seven federal district judges, to review and approve surveillances capable of monitoring United States persons [1] who are in the United States.

The Senate Intelligence Committee's report recommending favorable action on FISA set forth two objectives for the Act—to enhance U.S. intelligence capabilities and to protect constitutional rights. The report described FISA as designed to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." The Committee expected that FISA "would allow electronic surveillance in circumstances where, because of uncertainty about the legal requirements, the Government may otherwise be reluctant to use this technique for detecting dangerous foreign intelligence and terrorist activities by foreign powers in this country." The Committee has stated that the safeguards in FISA "may reasonably be expected to prevent any recurrence of the abuses of the past." S. Report No. 95–701, p. 16. Through its oversight activities since 1978, the Committee

[1] The Act defines "United States persons" to include U.S. citizens, lawfully admitted permanent resident aliens, and domestic organizations or corporations that are not openly acknowledged to be directed and controlled by foreign governments. § 101(i).

has sought to assess the effectiveness of the Act in achieving these objectives.

This is the fifth and final annual report of the Committee required by the congressional oversight provisions of FISA.[2] Unlike previous reports, this report reviews how the Act has worked since it went into effect. As the Committee stated last year regarding the final report required by the Act:

> This report will provide the Committee an opportunity to sum up its experience with implementation of the provisions of the Act over five years. The Committee expects to review that experience and prepare both a public report and a classified report on how the Act has worked in practice. The report will also describe any changes that may be needed in the Act itself and in the implementing procedures and policies of the relevant agencies. Related techniques such as physical search could be included in this review, and Committee hearings on possible amendments may be desirable.

The Committee has followed this plan. The Subcommittee on Legislation and the Rights of Americans held two closed hearings on FISA and an additional closed hearing on FBI guidelines which covered physical search techniques. At these hearings, the Subcommittee heard testimony from both policymakers and working-level officials of the principal agencies involved—the Department of Justice, the FBI, and the National Security Agency. The presiding judge of the FISA Court, Honorable John Lewis Smith, Jr., U.S. District Court, District of Columbia, and his predecessor, the late Honorable George L. Hart, Jr., Senior Judge, U.S. District Court, District of Columbia, also testified before the Subcommittee. The hearings were supplemented by written questions and staff briefings. The Subcommittee also asked witnesses who testified at the hearings on FISA in 1976–77 to submit any views they might have on the Act. Finally, the Committee received the regular semiannual reports from the Attorney General for the periods July-December, 1982, January-June, 1983, and July-December, 1983, supplemented by staff briefings. Based on these oversight efforts, the Subcommittee prepared the following unclassified report, A separate classified report has been submitted to the Executive Branch.

II. Contribution of FISA Surveillance to U.S. Intelligence Capabilities

The first question about FISA is whether it has, in fact, made a significant contribution to meeting U.S. foreign intelligence and counterintelligence requirements. The number of applications approved by the FISA Court has risen from 319 in 1980 (the first full calendar year after the Act took full effect) to 431 in 1981, 475 in 1982, and 549 in 1983.

[2] § 108(a) requires the Attorney General to fully inform the House and Senate Intelligence Committees on a semiannual basis concerning all electronic surveillance under FISA. § 108(b) requires the House and Senate Intelligence Committees to report annually for the first five years after the effective date of the Act concerning its implementation. Such reports must include an analysis and recommendations concerning whether the Act should be amended, repealed, or permitted to continue in effect without amendment.

To understand the Act's impact, it is necessary to know something about the surveillance methods used by the U.S. Government. More than just conventional telephone taps and hidden microphones are involved. FISA defines four categories of electronic surveillance:

Wiretaps—§ 101(f)(2). Unconsented acquisition by a surveillance device of the contents of a wire communication to or from a person in the United States, if the acquisition occurs in the United States. This includes not only voice communications, but also teleprinter, telegraph, facsimile, and digital communications. International communications are covered if one party is in the United States and the acquisition occurs in the United States.

Radio Intercepts—§ 101(f)(3). Intentional acquisition by a surveillance device of a radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States. This covers surveillance of wire communications while they are transmitted over radio-microwave links. International radio-microwave links are not covered by FISA. If domestic radio-microwave communications are acquired "unintentionally", § 106(i) requires that the contents be destroyed upon recognition unless they indicate a threat of death or serious bodily harm.

Monitoring Devices—§ 101(f)(4). Installation or use of a surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. Such devices may include microphone eavesdropping, surreptitious closed-circuit television (CCTV) monitoring, transmitters that track movements of vehicles, and other techniques. In some cases, the question of whether a device is covered by FISA depends on the circumstances of its installation or use.

Watch Listing—§ 101(f)(1). Acquisition by a surveillance device of the contents of wire or radio communications sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that person under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. Such targeting may involve acquisition of the contents of international communications of U.S. persons.

If a technique is on the borderline of the definition of electronic surveillance in FISA, the Justice Department resolves the issue following any precedents established by the FISA Court (if there are conflicting decisions by other federal courts in criminal cases). FISA does not cover electronic surveillance of U.S. persons who are abroad, nor does it apply to "watch-listing" that targets the international communications of foreign nationals who are in the United States. Moreover, FISA does not apply to physical search techniques that would require a warrant for law enforcement purposes, but do not fit the FISA definition of electronic surveillance. Such other intrusive techniques are not authorized by statute for intelligence purposes, but may

be used under procedures approved by the Attorney General pursuant to Executive Order 12333.

The National Security Agency and the Federal Bureau of Investigation are the two principal agencies that employ electronic surveillance under FISA. Certain activities covered by FISA have also been conducted by the Central Intelligence Agency, the Army, the Air Force Office of Special Investigations, and the Secret Service. The CIA is precluded by Executive Order from engaging in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance (Sec. 2.4(a) of E.O. 12333). The Secret Service performs defensive "sweeps" that may meet the definition of electronic surveillance in FISA. As with testing and training, a special provision of FISA permits such surveillance, under procedures approved by the Attorney General. These techniques may not be targeted against the communications of any particular person, and information acquired for a "sweep" may be used only to enforce Title III of the Omnibus Crime Control and Safe Streets Act of 1968 or the Communications Act of 1934, or to protect information from unauthorized surveillance. (§ 105(f)(2).)

NSA states that FISA "has achieved its major goal of providing clear legal authority for [this] foreign intelligence collection and of protecting the rights of United States persons." A senior NSA official identified specific benefits from FISA:

> The most important aspect of FISA is that it constitutes Congressional sanction for a variety of . . . foreign intelligence operations. Prior to FISA, the Executive Branch conducted these operations solely on the authority of the President. As you know, that authority was increasingly questioned and the prospect of numerous officials being sued in their private capacity was growing apace. Since enactment, the concern for personal liability has substantially receded so long as officials adhere to the terms of the Act.

NSA's general evaluation of FISA standards and procedures is also positive. The NSA official stated: "In particular, the operation of the approval process has been efficient and timely, and the security of the Foreign Intelligence Surveillance Court has been first-rate." The problems that NSA has had with certain technical requirements of the Act are discussed later. NSA officials consider those problems less important than the overall benefits resulting from FISA.

FBI Director Webster offered a favorable overall evaluation of FISA's impact on the FBI:

> . . . [O]ver the past four years, we have had occasion to test most aspects of the statute and have found them to permit necessary intelligence collection. We are convinced that it provides our personnel with the assurance that their activities today will withstand challenge in the future.

FBI officials were defendants in numerous lawsuits based on pre-FISA surveillance. A senior FBI official recalled the circumstances before passage of FISA:

> The various telephone company affiliates and other communications common carriers were increasingly uncertain of their liability in providing assistance without some judicial or statutory authority, and the District Court decision in *Truong-Humphrey* placed a limitation on inherent powers of the President once there was a focus on prosecution.
>
> You can add to this the more subtle effect of court action against former FBI officials and the resulting uncertainty on the part of our counterintelligence agents about their own liability which may arise from warrantless Fourth Amendment activity.

The number of FBI surveillances has steadily increased since May, 1979, when FISA went into effect.

The senior FBI official denied that FISA had "opened the flood gates of electronic surveillance" by the FBI. He testified that the increase since 1979 was due to other factors than the existence of FISA:

> While there may be some satisfaction with the FISA process that tends to stimulate more requests for coverage, it is the opinion of our operational personnel that the increase is a combination of our greater emphasis on electronic surveillance necessitated by more cautious hostile foreign intelligence services and the enhanced resources that made such an increase possible.

A major impact of the statute was to lift the virtual moratorium on surveillance of U.S. persons that had existed since 1976, when Attorney General Levi announced that no U.S. citizen was being targeted with warrantless wiretaps for intelligence purposes.

III. Effectiveness of Review of FISA Surveillance

The procedural requirements of FISA provide for several levels of review of each surveillance. The question for oversight is whether this review is conducted with adequate care, taking the necessary legal and policy considerations into account. FISA surveillance proposals undergo review within the originating agency and in interagency consultations, before they are approved for submission to the Attorney General or the FISA Court. The separate review practices for NSA and FBI surveillances are described below. The role of the FISA Court is then discussed. Finally, special attention is given to implementation and review of "minimization procedures" that limit collection and use of information about U.S. persons and to renewals of surveillance authorizations.

A. EXECUTIVE BRANCH REVIEW OF SURVEILLANCE PROPOSALS

The Committee has examined in detail the practices of the Executive branch for review of FISA surveillance proposals. In 1977, testimony indicated that NSA surveillances approved by the Director of Central Intelligence were considered at meetings of an interagency panel that included representatives of the CIA, State Department, Defense Department and others. Recent practice is less formalized than in 1977, but such surveillance proposals get careful attention. The Director or Deputy Director of Central Intelligence personally considers each proposal, based on the interagency panel's review. Proposals approved by the DCI are submitted to the Attorney General.

As appropriate, the CIA's Office of General Counsel, the Defense Department General Counsel's office, and the General Counsels' offices of particular agencies review legal questions raised by surveillance proposals. The legal issues appear to be raised early in the review process and handled professionally by these offices and by Justice Department attorneys. The Justice Department helps sort out the legal implications of more difficult cases, such as targeting individual U.S. persons or fitting new technology into the categories of the law.

In several cases, potential surveillance targets have held dual U.S. and foreign nationality. In order to target a U.S. person, FISA requires evidence of the person's involvement in clandestine intelligence activities, sabotage, or terrorism for or on behalf of a foreign power. Where that standard could not be met, potential intelligence would be lost.

A temporary legal constraint resulted from the Justice Department's interpretation of § 102(a) of FISA, which governs the narrow category of surveillance directed exclusively at foreign power communications and authorized by Attorney General certification rather than Court order. The Court order provisions of FISA refer to the use of "physical entry" to implement surveillance, but § 102(a) does not. The use of unconsented physical entry for § 102(a) surveillance purposes was not explicitly addressed when FISA was passed. In 1980 Attorney General Civiletti advised Congress of his opinion that FISA provided no authority for a "physical entry" to implement § 102(a) surveillance. However, in 1981 Attorney General Smith provided Congress with the results of a review of the law by the Justice Department's Office of Intelligence Policy and Review (OIPR), which concluded that FISA provided implied authority for "physical entry" under § 102(a).[3]

FBI surveillance proposals are reviewed by an FBI Headquarters supervisor, who prepares a memorandum from the FBI Intelligence Division to the Justice Department. This memorandum is sent both to the FBI Director's office and to the Justice Department's Office of Intelligence Policy and Review (OIPR). Some proposals are stopped or revised within the FBI before the Justice Department responds to them. Director Webster testified:

> My personal staff and I carefully evaluate every application for electronic surveillance. Our legal counsel division is involved in every step of the process. Polishing and shaping of the applications occurs as the paper work moves through the approval mechanism. . . . The net result is the best possible product for presentation to the Court.

[3] Further discussion is contained in Select Committee on Intelligence, "Implementation of Foreign Intelligence Surveillance Act of 1978–1979–1980" (Sen. Rept. 96–1017, October 30, 1980), pp. 6–7; and 1980–81 (Sen. Rept. 97–280, November 24, 1981), pp. 6–8.

The major review of FBI proposals occurs in informal consultation between the FBI and OIPR. It is assumed that an OIPR recommendation against a proposal will result in its rejection by the Attorney General, so OIPR's concerns carry great weight with the FBI.

The Justice Department reviews FBI proposals carefully. The Attorney General must approve the application to the FISA Court, presenting sufficient facts to support probable cause to believe that the target is a foreign power or an agent of a foreign power. OIPR insists that the FBI gather information through less intrusive techniques where feasible, before using electronic surveillance. Examples of cases in which no electronic surveillance was ever approved were reviewed by the Committee. They confirm this general description of the care taken in reviewing applications.

Once the informal review of FBI proposals is completed, the formal application goes to the FBI Director for signature and the Attorney General for approval. There are rarely any problems once the informal review is done. Applications signed by the Director, all of which are also recommended by OIPR by this time, are virtually always approved by the Attorney General for submission to the FISA Court.

Application papers for FBI surveillances are voluminous and would appear, on first impression, to impose significant paperwork burdens. Director Webster testified, however, that, "while it may be suggested that the pleadings are lengthy, I believe it is preferable to err on the side of an abundance of information." The Counsel for Intelligence Policy stated that the use of word processing equipment eases the burden considerably, because some of the language in the applications is standard recitation of information required under the law, with names and other identifying data inserted. Committee examination of actual applications confirms that the lengthy materials concern substance: probable cause; minimization (unless standard procedures suffice); and the nature of the information sought.

The review process sometimes must function under urgent time deadlines. FISA permits surveillance for up to 24 hours with Attorney General approval, rather than a Court order, in emergency situations. The Counsel for Intelligence Policy observed:

> The Attorney General can approve . . . coverage in an emergency situation. We have done it. It is possible to do. But as you look at the collection of signatures . . . the number of people that have to review and sign these things—you can imagine the fun. And some of them are 40 pages long in typing. So you can imagine what it is like once we get the emergency authorization, which may be verbal, to then reduce that to writing, get it through all those lawyers and past all those Cabinet officers and to the Court and signed in 24 hours. But we can do it and we have done it.

The FBI states that it has not postponed or delayed any surveillance because of the 24-hour filing requirement, although NSA has done so in at least one case.

All indications are that the review process conducted by the FBI and OIPR works well. That process clearly depends on the cadre of experienced personnel who have reviewed these applications since pre-FISA days. While FBI agents move from one assignment to another, the review personnel have provided essential continuity and experience. In future years, the quality of FISA implementation will depend upon the ability of these offices to recruit and train new highly qualified personnel to continue this critical supervision.

B. THE FOREIGN INTELLIGENCE SURVEILLANCE COURT

Most FISA proposals must be submitted to the Foreign Intelligence Surveillance Court (referred to here as the FISA Court). The only exceptions are those FISA surveillances directed solely at communications used exclusively between or among foreign powers, those that acquire technical intelligence and do not pick up spoken communications, and strictly limited testing, training, and defensive "sweep" practices.

The Justice Department summarized FISA Court operations as follows:

> On regularly scheduled court days, applications approved by the Attorney General are delivered to the clerk of the FISA Court with copies for the judge and the court's legal advisor. They review them in chambers. When court convenes, the applicant and the attorney who prepared the application appear before the court, answer any questions it may have, and swear to the contents of the application. If satisfied, the court signs the order or orders appended to the application. After the clerk has recorded the order and affixed the seal of the court, the order is returned to the applicant agency for execution. Normally the court is scheduled to sit one or two days twice a month. Applications requiring action in between scheduled court days are presented to one of two local judges who are members of the court.
>
> Orders issued for electronic surveillance of foreign governments or entities openly controlled by them or factions of foreign nations may approve surveillance for up to one year. All others may last no longer than 90 days, subject to renewal by the court. By statute, each order must direct compliance with the minimization procedures which accompany the application. These procedures, which have been adopted by the Attorney General, are designed to ensure that information about U.S. persons which is not pertinent to the foreign intelligence sought is not acquied, retained or disseminated.

The current and former Chief Judges of the FISA Court both testified that they have never found any serious problem with an application for a FISA surveillance. No application to the Court for an electronic surveillance has been rejected, although at least one was modified because the judge insisted upon a broader review of the circumstances in which use of a surveillance device required judicial approval.

This does not mean that the FISA Court does not pay attention to the proposals. The Court employs an experienced legal officer who reviews each application and discusses it with the judge (or judges)

hearing the request. Both the legal officer and the judges have on occasion raised questions regarding the sufficiency of information provided in an application, and sometimes additional information has been required. The FISA Court has also approved changes in the minimization procedures from time to time.

A major purpose of FISA was to ensure that electronic surveillance would not be directed against U.S. persons because of lawful political activities protected by the Constitution. Section 105(a)(3)(A) of the Act provides that no U.S. person may be targeted "solely upon the basis of activities protected by the first amendment. . . ." However, the standards for the finding of probable cause to believe that a U.S. person is an agent of a foreign power allow more flexibility than under criminal law enforcement procedures, in order to deal with clandestine intelligence activities on behalf of foreign powers and with international terrorism.

The Committee reviewed selected FISA applications to examine the evidence supporting the Court's probable cause finding in surveillance of U.S. persons. The criteria for selection included several types of U.S. person cases. The Committee continues to be informed, moreover, regarding every FISA case involving a U.S. person. Based on the materials reviewed by the Committee, the record indicates compliance with the probable cause requirements of the Act and the prohibition against targeting U.S. persons solely on the basis of constitutionally protected political activities. In one case, electronic surveillance of a U.S. person did not result in the acquisition of intelligence, because of a mistaken identity; such errors are extremely rare and probably unavoidable.

The FISA Court appears to perform its duties conscientiously, and there is testimony that its judges gradually develop experience in electronic surveillance matters. The fact that the Court has retained an experienced attorney as legal advisor and has given him an active role in reviewing the cases helps ensure proper attention to the applications. At the same time, however, there are limits to the oversight that one can expect the Court to undertake. The FISA Court is especially trusting with regard to implementation of minimization procedures, as indicated below. This makes it even more important to ensure that the Justice Department and other Executive branch agencies maintain high standards of care in proposing and implementing FISA surveillances.

C. MINIMIZATION REVIEW

Minimization is the process by which NSA and the FBI minimize unnecessary acquisition, retention, and dissemination of "nonpublicly available information concerning unconsenting United States persons." Under § 105 of the Act, the Court must determine that proposed minimization procedures for each surveillance meet the statutory definition and must order that the minimization procedures be followed. FISA minimization is significantly different from minimization in law enforcement cases. FISA minimization emphasizes the destruction of nonpertinent voice recordings or other communications texts in order to reduce the risk of future misuse of private information about U.S. persons. By contrast, law enforcement procedures require the retention of all recordings because of their possible use as

evidence. (The FBI has not been able to implement FISA minimization fully, because a Federal Court has suspended FBI records destruction pending the outcome of a lawsuit by historians and others challenging FBI records destruction criteria.)

Standard minimization procedures have been developed by the Justice Department with the FBI and NSA, and then adopted by the Attorney General with FISA Court approval. They are similar to procedures that were in effect before passage of FISA. Since each of the different types of surveillance operations run by each agency raises similar minimization concerns, it made sense to prepare a standard set of procedures for each type of operation. For example, there are standard procedures for FBI surveillances of foreign powers and different standard procedures for FBI surveillances of individual foreign agents. The procedures are tailored to the operational requirements and privacy considerations involved in each type of operation. Standard FBI procedures require the Bureau to develop criteria for each surveillance that distinguish pertinent and non-pertinent communications. All the standard procedures have been provided to the Select Committee on Intelligence. Redacted versions of the most common procedures were released following an FOIA request in 1980 and published in the Rutgers Law Journal (Vol. 12:496–507, Spring 1981).

When the original procedures were being formed and tested after FISA went into effect, the FISA Court contributed to their refinement. More recently, however, the Court does not appear to have raised any matters leading to further changes. The Justice Department has occasionally found flaws in the procedures and has proposed changes that were then approved by the Court.

Implementation of the minimization procedures is left to the implementing agencies, subject to periodic review by the Justice Department. NSA takes positive minimization actions wherever this is technically feasible. For example, a senior NSA official testified:

> . . . with the exception of Executive Branch officials, the identity of United States persons is rarely disseminated when a report is issued. The usual practice is to wait for a recipient to request specific identities and then provide the identity, if adequate justification exists to invoke one of the several criteria that permit dissemination of the identity.

Testimony indicates that NSA has applied these procedures when dealing with requests from policymakers, as well as from elements of the intelligence community.

A senior FBI Intelligence Division official testified that the FBI continues "to emphasize to our monitors and translators the meaning and importance of minimization, particularly the importance of minimization of acquisition." The Counsel for Intelligence Policy noted that in three criminal prosecutions of targets of FISA surveillance, defendants have challenged FBI minimization and that in each case the court found the minimization procedures to be in compliance with the Act. The full FBI logs segregating pertinent from nonpertinent conversations—and, in at least one case, the full surveillance tapes—have been provided to courts and defendants when FISA surveillance was used in a prosecution.

The Justice Department's Office of Intelligence Policy and Review also engages in periodic in-depth reviews of both NSA and FBI compliance with minimization procedures. OIPR attorneys personally visit major FBI offices and NSA to inspect pertinent records and to discuss minimization practices with agency personnel who must implement them.

Finally, § 105(d)(3) of the Act allows the FISA Court to "assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated." Both FISA Court Judges and OIPR personnel testified, however, that the Court does not make an effort to assess compliance beyond asking occasional questions. The Court has not, for example, examined any OIPR reports on the review of agency performance. Proper minimization, both in formulating procedures and in implementation, appears to depend almost exclusively on the implementing agencies and OIPR. It is reassuring that these agencies seem to be handling minimization in a very professional manner responsive to the language and intent of the Act. On several occasions, the Department of Justice has reported to the Court technical violations of the minimization procedures and other provisions of the Court order, such as failure to terminate a surveillance immediately when an order expired. The solution to these problems has been to place the improperly acquired information under Court seal.

D. EXTENSIONS OF SURVEILLANCE ORDERS

Under § 105(d) of FISA, surveillances of most foreign powers may be authorized for up to one year before renewal; all other surveillances may be authorized for no more than 90 days before renewal. Extensions of orders may be granted on the same basis as an original order. Applications for extensions are subject to agency review procedures, interagency reviews, and review by the FISA Court. Agencies may also conduct internal operational reviews apart from requests for extensions of FISA orders.

The 90-day renewal requirement for surveillance of individuals has caused some problems for the FBI in cases involving hostile intelligence officers. Sometimes the surveillance has been interrupted when the 90-day period expired before a renewal order could be obtained. A senior FBI Intelligence Division official states that the 90-day renewal requirement "does not interfere at the present time with our ability to collect" and that "it is not more than an inconvenience at the present time." The Counsel for Intelligence Policy testified that, because of cases "where coverage would lapse between renewals because of delay in the total process," the Justice Department and the FBI "have had to streamline the procedure." She explained that in foreign official cases, "the probable cause is fairly easy to establish" and "renewals do not take a lot of complex scrutiny." With the use of word processing equipment, the retyping of the renewal application now takes less time "because you are just adding updated facts to a statement of facts already there."

Applications to the FISA Court for extensions indicate what previous orders have been granted and the judge or judges involved, but otherwise little new information appears to be added apart from updating the facts supporting probable cause. A renewal application may note the possibility of proceeding to prosecution and explain why, despite this possibility, the continuing foreign intelligence purpose and value of the information sought justifies continued use of FISA rather than Title III procedures. The judges' times of service are so arranged that a judge rarely handles the extension of an order that he had approved earlier. Consequently, the judge reviewing an extension request considers it as he would an original application.

The FISA Court thus subjects renewal applications to a de novo review of whether the legislated criteria for a court order are met, but it does not oversee the conduct of those surveillances. Chief Judge John Lewis Smith, Jr., assured the Committee "that the interests of individual American citizens and foreign alien residents are fully protected [because] the minimization procedures go all the way to protect their rights." It is left to others to examine how the FISA Court's orders are implemented.

E. REVIEW IN SUBSEQUENT JUDICIAL PROCEEDINGS

Several FISA surveillances have been reviewed by other federal courts in the context of criminal prosecutions. The most significant issue to arise in these cases is the question of whether the surveillance was improperly conducted for law enforcement rather than foreign intelligence purposes. The Justice Department has advised:

> Whether it makes any difference if criminal prosecution is contemplated when a FISA surveillance is authorized is an unresolved legal issue. Clearly FISA surveillances must have an intelligence purpose. (§ 104(a)(7).) It is equally clear that the product of the surveillance can be used in criminal proceedings. (§ 106(c).) One judge has held that intelligence need not be the primary purpose of the surveillance so long as it is a purpose. *United States vs. Falvey*, 540 F. Supp. 1306, 1314 (E.D.N.Y. 1982), cited with agreement, *In Re Grand Jury Supoena of Martin Flanagan*, 691 F. 2d 116 (2nd Cir. 1982). Another judge viewed the FISA Act itself as requiring that intelligence be the *primary* (but not sole) purpose of of the surveillance. *United States* v. *Megahey*, 553 F. Supp. 1180, 1189–90 (E.D.N.Y. 1982). No court that has reviewed FISA applications in criminal cases has found them defective in regard to the purpose, regardless of whether a "primary purpose" test has been applied.

The fact that every court which has considered this matter has found the use of FISA to be proper does not necessarily resolve all concerns in this area. One question is to what extent the FBI can use FISA surveillance to obtain both foreign intelligence information and criminal evidence for prosecution purposes. The FBI's alternative is to be limited to the criminal law enforcement procedures of Title III

of the Omnibus Crime Control Act of 1968 when criminal prosecution is known to be a likely outcome.[4]

Warrantless surveillance in the United States conducted before FISA, to whatever extent it may be permissible under the Constitution, was subject to limits if prosecution was intended. As Judge McLaughlin said in the *Falvey* case:

> [S]everal courts have ruled that, while warrantless electronic surveillance is permissible when the purpose of the surveillance is to obtain through intelligence information, nevertheless, when the purpose of the surveillance is to obtain evidence of criminal activity, that evidence is inadmissible at trial.
>
> In *Truong*, for example, the Executive Branch had conducted warrantless wiretaps pursuant to its "inherent power." The Government admitted, however, that the "primary" purpose of the investigation had shifted from that of obtaining foreign intelligence information to that of obtaining evidence of a crime. The District Court admitted the wiretaps in a criminal crime. The District Court admitted the wiretaps in a criminal prosecution that were obtained while the primary object was foreign intelligence information but excluded those obtained after the focus of the surveillance became evidence of criminality. In doing so, it rejected the Government's argument "that, if surveillance is to any degree directed at gathering foreign intelligence, the executive may ignore the warrant requirement of the Fourth Amendment." The bottom line of Truong is that evidence derived from warrantless foreign intelligence searches will be admissible in a criminal proceeding only so long as the primary purpose of the surveillance is to obtain foreign intelligence information.

Judge McLaughlin went on to say, however, that all evidence derived from an electronic surveillance pursuant to a FISA Court order would be admissible. He based his ruling upon the text and legislative history of FISA, stating, "In enacting FISA, Congress expected that evidence derived from FISA surveillances could then be used in a criminal proceeding." [5]

FISA does indeed contemplate the possible use in criminal proceedings of information derived from electronic surveillances. The

[4] Title III requires that applications be made to regular federal District Courts, rather than to a single, national court with special security procedures. Title III also requires that an application show probable cause to believe that the target has committed, is committing, or is about to commit a specific federal crime. FISA does not require a criminal standard for surveillance of foreign officials or members of international terrorist groups who are not U.S. persons. In addition, the probable cause standard in FISA for surveillance of U.S. persons permits surveillance in terrorism cases where the crime involved occurs abroad, if there is an equivalent offense under U.S. federal or state law. The "minimization" requirements in Title III are tied to criminal law enforcement, while the comparable provisions of FISA are designed to meet intelligence needs. And unlike Title III, FISA establishes specific *in camera, ex parte* procedures for review of the legality of surveillance in subsequent judicial proceedings.

[5] *United States* v. *Falvey*, 540 F. Supp. 1306, 1314 (E.D.N.Y. 1982).

Committee's 1978 report accompanying FISA recognized, moreover, that FISA surveillance would be:

> . . . part of an investigative process often designed to protect against the commission of serious crimes such as espionage, sabotage, assassination, kidnaping, and terrorist acts committed by or on behalf of a foreign power. Intelligence and law enforcement tend to merge in this area.

The report made a particularly strong case in the counterintelligence area, noting that "foreign counterintelligence surveillance frequently seeks information needed to detect or anticipate the commission of crimes." In a later passage, however, the report stated that "the primary purpose of electronic surveillance conducted pursuant to this chapter will not be the gathering of criminal evidence." (Sen. Rept. No. 95–701, pp. 11 and 62.) Variations in judicial interpretations are thus not surprising.

The most recent decision on this issue is that of the Court of Appeals for the Second Circuit in the *Megahey* case. The Court stated that "[t]he requirement that foreign intelligence information be the primary objective of the surveillance [under FISA] is plain." But the Court also stated:

> . . . we emphasize that otherwise valid FISA surveillance is not tainted simply because the government can anticipate that the fruits of such surveillance may later be used, as allowed by § 1806(b), as evidence in a criminal trial.

Turning to the role of the judiciary, the Court of Appeals stated that the Executive branch certification to the FISA Court as to the purpose of the surveillance is subject "to only minimal scrutiny by the courts." The Court also indicated that, on the question of the validity of the certification, a court reviewing this issue in a subsequent proceeding has "no greater authority to second-guess the executive branch's certifications than has the FISA Judge." The Court noted, however, that the reviewing court could grant a hearing on the validity of such certifications if presented with evidence that the surveillance was based on fraudulent representations to the FISA Judge.[6]

Thus, courts remain divided over whether a "primary purpose" test is required by the law. And it is left largely to the Executive branch to determine, in individual cases, when its purpose is to obtain foreign intelligence information and when it is to prosecute criminals. This leaves the FBI and Justice Department with difficult choices and responsibilities.

The difficulty of determining whether FISA or Title III is the appropriate procedure for a surveillance approval is greatest with regard to some investigations of international terrorism. The version of FISA that was finally enacted did not limit targets to international terrorists who operate primarily abroad or on behalf of a foreign government (and who would be targeted almost always primarily to obtain foreign intelligence information). Rather, any terrorist group or its agents may be targeted if their violent activities "transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum." (§ 101(a)(4) and (c)(3)). Thus, it is conceivable that FISA surveillance could be directed at persons whose activities are essentially a domestic law enforcement problem, even though they have international ramifications or connections. In the FBI, investigations of both domestic and international terrorism are supervised by the Criminal Investigative Division, not the Intelligence Division, partly because criminal prosecution is a major thrust of the FBI's overall counterterrorism program. There is a clear need for caution, therefore, in cases that appear to be more concerned with domestic law enforcement than with foreign intelligence collection. The Committee believes that the Justice Department should use Title III when it is clear that the main concern with respect to a terrorist group is domestic law enforcement and criminal prosecution, even if the surveillance will also produce some foreign intelligence information.

Apart from this issue, the courts that have undertaken subsequent review of FISA surveillances in criminal cases have been satisfied with the statute and its implementation. In an opinion by Judge Wilkey, joined by Judges Bork and Scalia, the Court of Appeals for the District of Columbia Circuit has observed, "In FISA Congress has made a thoroughly reasonable attempt to balance the competing concerns of individual privacy and foreign intelligence." The Court went on to credit FISA for assisting the judiciary in conducting subsequent reviews:

> If anything, the legality inquiry mandated by FISA is easier for a court to perform ex parte than the pre-FISA inquiry into the legality of warrantless electronic surveillance. Previously, courts had to determine whether the surveillance fell within the President's inherent power to conduct electronic surveillance for foreign intelligence purposes. The FISA inquiry at issue here is merely to determine whether the application and order comply with the statutory requirements. In this case it is evident that they do. Furthermore, . . . FISA incorporates nonjudicial safeguards [i.e., Executive branch controls and congressional oversight] to ensure the legality of the surveillance.[7]

In this case, the criminal defendants had been overheard on a surveillance that had nothing to do with their prosecution. Such cases arise with some regularity and thus provide another forum for judicial examination of FISA implementation.

The role of the courts under FISA is not, therefore, limited to the prior review of applications and extensions by the FISA Court. Other Federal courts have an opportunity to consider relevant aspects of FISA surveillances that bear directly or indirectly upon criminal prosecutions, including the implementation of minimization procedures.[8]

---

[6] *United States* v. *Megahey*, No. 83–1313, 2d cir., August 8, 1984.

[7] *United States* v. *Belfield*, 692 F.2d 141 (D.C. Cir. 1982).

[8] In the *Belfield* case, the Court of Appeals specifically determined "that the minimization procedures approved in the original order have been followed." Judges in other cases have also been provided the materials needed to evaluate implementation of minimization procedures. See above, p. 19.

In the *Megahey* case, the Court of Appeals stated that "a reviewing court is to have no greater authority to second-guess the executive branch's certifications than has the FISA Judge." The Court went on, however, to review the *in camera* submissions to the FISA Judge and to reaffirm the District Court's finding that the government's certification regarding the purpose of the surveillance was accurate "both initially and throughout."

As such cases continue to arise, the courts are building a body of public judicial precedents on matters of FISA interpretation. While the FISA Court conducts its business almost entirely in secret, the combination of subsequent judicial review by other courts and congressional oversight is a safeguard against the risk of possible reliance on a body of precedents that might amount to "secret law."

IV. Other Techniques Governed by the Fourth Amendment

FISA established statutory procedures for only some of the intrusive techniques that are subject to the judicial warrant requirement of the Fourth Amendment when employed for law enforcement purposes. In enacting FISA, Congress did not address the question of whether techniques outside the scope of FISA electronic surveillance should be used for intelligence purposes—with or without a court order—inside the United States or against U.S. persons abroad. With regard to physical searches, for example, the report of the Senate Intelligence Committee stated:

> Although it is desirable to develop legislative controls over physical search techniques, the committee has concluded that these practices are sufficiently different from electronic surveillance as to require separate consideration by the Congress. S. 2525, the National Intelligence Reorganization and Reform Act of 1978, addresses the problem of physical searches within the United States or directed against U.S. persons abroad for intelligence purposes. The fact that [FISA] does not cover physical searches for intelligence purposes should not be viewed as congressional authorization for such activities. In any case, the requirements of the fourth amendment would, of course, continue to apply to this type of activity.

The Committee also noted that Executive Order 12036, the predecessor to Executive Order 12333, "places limits on physical searches and the opening of mail." The report made similar observations about electronic surveillance of Americans abroad. (S. Rept. 95–701, pp. 35, 38.)

In 1978–80, the Congress considered statutory procedures for these other techniques as part of comprehensive intelligence charter legislation, such as S. 2525 (cited in the report on FISA) and the proposed National Intelligence Act of 1980. Charter provisions supported by the FBI in 1980 would have established procedures similar to FISA for physical searchers in the United States for intelligence purposes. By contrast, the proposal endorsed by the Executive branch for electronic surveillance and physical search of U.S. persons abroad differed substantially from FISA, although it retained a court order procedure. In the absence of legislation, the Executive branch has relied upon the position of the Justice Department that the President and, by delegation, the Attorney General have constitutional authority to approve these other techniques for intelligence purposes without either statutory authorization or a court order.

The Committee has sought information about the Intelligence Community's use of techniques other than FISA electronic surveillance

that would require a judicial warrant for law enforcement purposes. The Justice Department has agreed to inform the Committee fully with regard to any exercise of authority to conduct intelligence searches within the United States and searches abroad involving the property of U.S. persons. The Committee has also obtained information from the Justice Department and the operating agencies about electronic surveillance of U.S. persons abroad, as well as the surveillance of international communications of foreign nationals who are in the United States. These techniques are regulated by procedures approved by the Attorney General pursuant to Executive Order 12333. The Committee was given copies of the most recent revised procedures shortly before they took effect in 1982 (for CIA and the Defense Department) and in 1983 (for the FBI). Revised NSA procedures are being developed and will also be made available to the Committee.

Executive branch policies for intelligence searches and for overseas electronic surveillance are discussed separately below.

A. Intelligence Searches

Intelligence searches may include such techniques as surreptitious entry of private premises, opening sealed packages, and others. They raise difficult legal and policy issues, not only because of the absence of statutory authorization or a court order, but also because some types of search may be governed by federal law.

Section 2.5 of Executive Order 12333 delegates authority to the Attorney General to approve any type of intelligence search, as follows:

> The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order.

Since 1981, CIA and Defense Department procedures and FBI guidelines have been revised accordingly. In 1983, the FBI's guidelines incorporated definitions of "foreign power" and "agent of a foreign power" comparable to those in FISA for intelligence searches within the United States.

The Justice Department's Counsel for Intelligence Policy testified that the Attorney General approves FBI Intelligence searches "sparingly" and that each case receives "extremely close scrutiny within the FBI and the Department to ensure that the rights and interests of U.S. persons are fully protected." According to the Counsel and FBI Director Webster, the approval procedures are almost identical to the Executive branch review procedures for FISA surveillances.

The delegation to the Attorney General in Executive Order 12333 is limited by Section 2.8, which states:

> Nothing in this Order shall be construed to authorize any activity in violation of the Constitution *or statutes* of the United States. (Emphasis added.)

This provision places some restrictions on intelligence searches, although the extent of those limits is uncertain. Federal statutes expressly prohibit the opening of mail in U.S. postal channels without a judicial warrant.[9] Another federal statute makes it a crime for a federal law enforcement officer to search a private dwelling without a judicial warrant, except as incident to an arrest or with the consent of the occupant.[10] The Justice Department has submitted an opinion concluding that this statute "is not an impediment to properly approved warrantless physical searches for national security purposes," but the opinion also states that "the issue is not free from doubt." The question is whether legislation passed in 1921 should be considered "an anachronism" because its original purpose does not apply, as the opinion argues, or should be read literally to apply to FBI Agents who act as both law enforcement and counterintelligence officers.

The Justice Department has also provided to the Committee an analysis of the constitutionality of warrantless intelligence searches, with selected documents indicating how the Executive branch handled intelligence search issues before 1977. The constitutional problems with warrantless intelligence searches are generally the same as those raised by warrantless electronic surveillance before enactment of FISA. An analysis of this question prepared for the Subcommittee on Legislation and the Rights of Americans is found in the Appendix to this report.

Asked about the risks of civil or criminal liability for FBI agents, in light of the undecided constitutional issues, Director Webster testified:

> Well, we are fortified by considerable advice and opinion of the Attorney General as to the inherent authority of the President delegated to him to authorize searches in national security matters. That convinces me that the good faith defense is clearly available to us . . . in relying on the advice of our chief law enforcement officer. But I am also mindful of course that the *Keith* opinion in 1972 left open the questions of whether searches required a warrant in national security matters. I am sure our agents can withstand the lawsuits, but I naturally prefer not to have them at all.

Legislation similar to FISA for intelligence searches could resolve these constitutional and legal uncertainties. The Justice Department's analysis explains why ordinary judicial warrant procedures are not suitable for intelligence searches and discusses the problem of inadequate security arrangements for district courts and magistrates. The

[9] Relevant statutes include 18 U.S.C. §§ 1701–1702, 1703(b), and 39 U.S.C. § 3623(d).
[10] 18 U.S.C. § 2236. This misdemeanor statute was enacted in 1921 in response to reports of overly aggressive conduct by prohibition enforcement agents.

Supreme Court recognized this problem in the domestic security surveillance case and invited Congress to establish procedures by which "the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court." [11] Congress followed this guidance in framing FISA, and the experience under the Act suggests that similar search procedures would be workable. The Justice Department's analysis states:

> There is no comparable modified provision or procedure by which to obtain warrants authorizing physical searches conducted for foreign intelligence purposes. . . . The operation of the United States Foreign Intelligence Surveillance Court demonstrates that a properly structured and specialized court can achieve the expertise and security to consider these issues, and a properly drawn statute can prevent judicial intrusion into policy decisions legitimately left to the Executive Branch.

The Committee is persuaded that a court order procedure for physical searches in the United States, using either the FISA procedure or a procedure comparable to FISA, ought to be established. Based on the FISA experience, we are now confident that such a court order procedure would remove the legal and constitutional ambiguities inherent in current Executive branch practice regarding physical searches for foreign intelligence purposes. We also note that Executive branch approval standards for such physical searches are already very similar to FISA standards, and that previous use of the FISA Court (which was stopped when the Court ruled that it lacked authority in such cases) did not appear to have caused any practical difficulties.[12] The Committee intends to develop a legislative proposal for an amendment of FISA or for a court order procedure comparable to FISA, in consultation with the Attorney General.

Pending consideration and passage of such legislation, the legal position of the Committee and of Congress regarding warrantless physical search practices remains comparable to its position before FISA in the field of electronic surveillance, which was described in the *Keith* case as "essentially neutral." Congress has done nothing to authorize such actions by the Executive branch; any determination of the validity of Executive branch assertions of inherent powers to conduct warrantless physical searches is up to the courts.[13]

The Justice Department's physical search analysis also raises the "primary purpose" issue of intelligence versus prosecutorial goals, discussed earlier regarding FISA surveillances. Various court decisions, including *Truong-Humphrey*, hold that the "primary purpose" of the search must be to gather foreign intelligence, in order to justify

[11] *United States* v. *United States District Court*, 407 U.S. 297, 322–323 (1972).
[12] In 1980 Attorney General Civiletti obtained FISA Court approval for three intelligence searches, but in 1981 the FISA Court ruled that it did not have authority to approve intelligence searches in the absence of legislation. The FISA Court did not address the question of the legality of warrantless intelligence searches. See Select Committee on Intelligence, "Implementation of the Foreign Intelligence Surveillance Act of 1978—1979–80" (Sen. Rept. 96–1017, October 30, 1980), pp. 9–19; and 1980–81 (Sen. Rept. 97–280, November 24, 1981), pp. 3–4 and 10–19.
[13] For the Supreme Court's discussion of the position of Congress on warrantless national security electronic surveillance before FISA, see *United States* v. *United States District Court*, 407 U.S. 297, 303–306 (1972).

a claim of constitutional authority to act without a judicial warrant.[14] The Justice Department explains the difficulties in complying with this requirement:

> The courts apply the "primary purpose" test to an investigation after it is completed, and their task is aided by evidentiary hearings and the full documentary record of the investigation. Unfortunately, it is substantially more difficult for the Executive to apply these standards in the midst of an investigation, when the "record" is not yet complete and the need for a quick decision may be substantial. Careful scrutiny of the purpose and motives of the investigation is necessary, as is the need to obtain as much information as possible so that the Attorney General may make an informed judgment on the purpose of the search. As is reflected in all three sets of procedures, the department requires that the purpose of a proposed physical search be to obtain foreign intelligence information.
>
> However, we do not believe that purpose must be subjected to qualitative assessments, such as whether it is "primary," "substantial," or "exclusive." It is certainly important to determine whether the case includes prosecutive potential or intentions. Nonetheless, it is our position that such a search may be approved so long as it is in furtherance of a legitimate and reasonable intelligence purpose. On the other hand, a search that may have only an insubstantial, but very troubling, criminal aspect may be disapproved, based on all the facts, despite a "primary" intelligence purpose.

This policy not to apply the "primary purpose" test used by the courts in cases such as *Truong-Humphrey* is cause for some concern, even though the Committee is not aware of any criminal prosecution involving an intelligence search since that case. The *Falvey* case makes clear that it is the court order in FISA that moves some judges to exempt electronic surveillances from the "primary purpose" test.[15] And the Court of Appeals in the *Megahey* case states that even a court-ordered FISA surveillance should have foreign intelligence information as its primary objective. Therefore, the Department of Justice analysis might well not be sustained in a court test. The Committee recommends that the Executive branch take these considerations into account in its review of proposals for warrantless physical searches.

B. ELECTRONIC SURVEILLANCE ABROAD

Current Executive branch policies for non-FISA electronic surveillance affecting Fourth Amendment rights and the interests of U.S. persons are substantially the same as first formulated under the Ford Administration. There have been slight revisions since then, but the overall framework has remained constant.

The approval procedures adopted under Executive Order 12333 are mostly similar to the Executive branch review procedures for FISA surveillance and intelligence searches. An important difference is the

[14] *Truong, supra,* 629 F. 2d at 915; *Humphrey, supra,* 456 F. Supp. at 58; *United States* v. *Butenko,* 494 F. 2d 593, 606 (3rd Cir.) *(en banc), cert. denied sub nom. Ivanov* v. *United States,* 419 U.S. 88 (1974).

[15] See above, p. 24.

definition of "agent of a foreign power" as it applies to U.S. persons abroad. The relevant Department of Defense procedures do not require a connection between the "clandestine intelligence activities" of the agent and possible federal law violation. Moreover, a U.S. person may be considered an "agent of a foreign power" and targeted for surveillance if he or she is a foreign official without any involvement in intelligence or terrorist activities. Another standard requiring no specific criminal conduct applies to a U.S. person in contact with a foreign intelligence service for the purpose of providing access to classified information to which such person has access. In some circumstances the procedures also permit targeting a U.S. person acting unlawfully in knowing concert with a foreign power, or a U.S. organization that is controlled indirectly by a foreign power.[16]

The Committee believes that standards for targeting electronic surveillance against U.S. persons abroad should, whenever practicable, be analogous to FISA standards, in light of the principle that a U.S. person who travels to a foreign country does not thereby cede the right to be free of undue electronic intrusion by his or her own government. The Committee recognizes that there are circumstances, such as the case regarding some U.S. persons who are also officials of foreign governments or factions thereof, in which different standards may be justified. And the difficulty of devising a court order system has prevented Congress from legislating with regard to overseas surveillances. But the Committee supports application of FISA-like standards in targeting electronic surveillance against U.S. persons abroad whenever this is practicable.

The greatest challenge to those responsible for oversight of intelligence surveillance operations has been to devise means to accommodate the privacy interests of U.S. persons given the technical capabilities of the SIGINT system to provide information based on topical interests. Without targeting any particular U.S. persons, SIGINT collection operations inevitably give NSA direct access to international and foreign communications of and about U.S. persons. Through a combination of internal NSA policies and procedures concurred in by the Attorney General, systematic efforts are made to minimize the acquisition, retention, and dissemination of private information about unconsenting U.S. persons.

The basic premise in minimizing acquisition is that communications obtained through SIGINT collection are not "acquired" by the Government, in any meaningful sense, unless and until they are processed for the human eye or ear. Thus, safeguards focus on the means used to select particular communications, from the collected intercepts, for analysts to receive. Selection criteria that result in the processing of communications of or about U.S. persons are, and must be, carefully assessed to ensure their foreign intelligence value.

The role of the courts in reviewing constitutional issues raised by SIGINT collection and other intelligence surveillance and search techniques abroad is extremely limited. One court decision regarding electronic surveillance of Americans abroad by Army intelligence has held that "prior judicial authorization is constitutionally required" in a case that "did not involve United States citizens who were agents

[16] See Procedure 5, Part 2.C.2.a. of the Procedures Governing DoD Intelligence Components that Affect United States Persons, December 1982 (DoD 5240.1–R). While these procedures are unclassified, procedures for CIA and NSA on this subject are classified.

of foreign powers or who were in possession of foreign intelligence information." This decision led to a consent agreement by the Army that it would comply with the court's ruling.[17] In cases challenging NSA surveillance, however, the courts have uniformly upheld the Government's argument that the "state secrets privilege" forecloses judicial redress for any Fourth Amendment violation involving sensitive SIGINT operations.[18] In one case where the Government admitted that NSA disseminated SIGINT information about the plaintiff to the FBI, the Court of Appeals for the Sixth Circuit refused to consider the merits of the Fourth Amendment issues raised by NASA "watch listing" because the sensitive information about NSA techniques could not be disclosed under the "state secrets privilege." [19]

Thus, except for the Army surveillance case which involved conventional wiretapping, the court decisions suggest that the courts are unlikely to consider whether Fourth Amendment rights have been violated by other forms of electronic surveillance abroad, including SIGINT operations. This problem could also arise under FISA, because the civil penalties in the Act for unlawful surveillance might be unenforceable if the Government successfully invoked the same "state secrets privilege" argument. However, § 106(f) of FISA provides a special procedure for *in camera* and *ex parte* judicial examination of sensitive materials "to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." This procedure was designed to accommodate both the Government's need to protect sensitive surveillance methods and the rights of citizens to a judicial determination of the legality of the surveillance. Without a similar statute for non-FISA surveillance, the courts have chosen not to adopt an *in camera* and *ex parte* review procedure on their own authority.

The Committee believes that it might be worthwhile to consider development of legislation to deal with the "state secrets privilege" in the context of lawsuits alleging violations of constitutional rights by non-FISA electronic surveillance or other techniques. Such legislation might reasonably be considered in conjunction with efforts to alleviate problems associated with the personal liability of federal officials.[20]

With the courts reluctant or unable to consider cases challenging the constitutionality of intelligence surveillance abroad, congressional oversight by the Intelligence Committees becomes especially important as the only check outside the Executive branch. The Committee believes such oversight would be enhanced by obtaining regular written reports on non-FISA electronic surveillance that affects Fourth Amendment rights, comparable to the semiannual reports submitted by the Attorney General under FISA. The Committee is requesting, therefore, that the Attorney General supplement his semiannual FISA reports with similar reports on the use of non-FISA search and surveillance techniques against persons in the United States or U.S. persons abroad that would require a warrant if used for law enforcement purposes. The Committee intends to work with the Inspectors General and General Counsels of NSA and any other relevant agencies to ensure that dissemination procedures are properly implemented and to improve congressional oversight of that implementation. The Committee will ask OIPR to assist it in this oversight, as appropriate.

[17] *Berlin Democratic Club* v. *Rumsfeld*, 410 F. Supp. 144, 156–157 (D.D.C. 1976); Joint Motion and Stipulation for Dismissal, *sub. nom. Berlin Democratic Club* v. *Brown*, Civ. No. 74–310 (April 4, 1980).

[18] *Halkin* v. *Helms*, 598 F.2d 1 (D.C.Cir. 1978); *Salisbury* v. *United States*, 690 F.2d 966 (D.C.Cir. 1982).

[19] *Jabara* v *Webster*, 691 F.2d 272 (6th Cir. 1982).

[20] See the discussion in *Litigating National Security Issues*, American Bar Association Standing Committee on Law and National Security, 1983, pp. 25–47.

The Committee has requested the results of OIPR's periodic reviews of compliance with FISA minimization procedures, and has received those reports for 1984. The Committee expects that NSA and all other agencies of the Intelligence Community will consult with it regarding search or surveillance issues that raise significant questions of legality or propriety.

V. Conclusions and Recommendations

The Committee has reviewed the five years of experience with FISA and finds that the Act has achieved its principal objectives. Legal uncertainties that had previously inhibited legitimate electronic surveillance were resolved, and the result was enhancement of U.S. intelligence capabilities. At the same time, the Act has contributed directly to the protection of the constitutional rights and privacy interests of U.S. persons.

The Committee seeks especially to allay any concern that the increase in electronic surveillance since enactment of FISA poses a danger to the privacy of U.S. persons. The number of applications approved by the FISA Court has steadily increased from 319 in 1980 (the first full calendar year after the Act went into effect) to 431 in 1981, 475 in 1982, and 549 in 1983. Based on a careful examination of the FISA process, including a detailed breakdown of these statistics and examination of the facts and circumstances in a variety of different types of cases, the Committee is convinced that this increase does not reflect any relaxation in strict protections for the privacy of U.S. persons. The applications submitted to the FISA Court that the Committee has examined show the utmost care in adhering to the requirements of the Act. While it is impossible to measure the precise contribution of the FISA Court to this result, the high quality of the applications indicates the value of independent judicial scrutiny in protecting privacy and civil liberties.

The Committee has been fully briefed on the number of U.S. persons who have been subjected to FISA surveillance, as well as the time periods and the methods involved and, in summary form, the justification for each such surveillance. The Committee is satisfied that the number involved is not excessive, that such surveillances of U.S. persons are not capricious, and that the requirements of the Act are being met.

Some technical problems have arisen with a few provisions of the Act as indicated in this report. None have caused such problems as to require modification at this time.

The current position of the Executive branch is that the Act should be permitted to continue in effect without amendment. This view was expressed at the Subcommittee hearings by the FBI Director, the Deputy Director of the National Security Agency, and the Counsel for Intelligence Policy in the Justice Department. Witnesses who testified

at the Committee's hearings on FISA in 1976–77 have been asked for their assessment of the Act. While several urged careful oversight of implementation of the Act and related issues, none suggested any specific amendments.

Since 1979, several amendments have been suggested to remedy actual or anticipated problems that may not have been fully appreciated at the time FISA was enacted. For example, in 1979, NSA proposed changing from 24 to 48 hours the length of time allowed for surveillance without a court order in emergency circumstances. Director of Central Intelligence Stansfield Turner proposed, at 1980 hearings on intelligence charter legislation, amendments to allow surveillance of U.S. persons who are dual nationals and serve as senior officials of foreign governments. He also proposed changing the standards to permit surveillance based on a person's status as a former senior foreign officials. In 1981 the Secret Service recommended clarifying the FISA provision for defensive "sweeps" to permit use of information indicating a threat of serious bodily harm. These proposals were reiterated by Director Casey on April 15, 1981. The Committee also finds some merit in a suggestion that the 90-day renewal period might be lengthened in cases of foreign government officials who act as intelligence officers in the United States.

Some technical revisions in FISA would appear warranted, especially if they could be considered without re-opening debate on the basic framework of the Act. The Justice Department and the agencies that conduct FISA surveillance do not now believe, however, that these comparatively minor problems justify amending FISA at this time. The Committee recommends therefore, that the Act should remain in effect without amendment until such time as the Executive branch submits new proposals for specific changes. The Committee would give the most serious consideration to any such proposals that do not affect the central features of the Act.

On the issue of intelligence searches, the Committee has recommended earlier in this report the development, in consultation with the Attorney General, of a legislative proposal to establish statutory procedures comparable to FISA for physical searches. Such a proposal would enable Congress to provide statutory standards and procedures for activities that are being carried out today solely on the basis of assertions of Presidential authority.

The Committee does not recommend legislation to extend the coverage of FISA to overseas surveillances. The practical differences between overseas surveillance and FISA surveillance make enactment of such legislation an extremely difficult enterprise. The Committee strongly recommends, however, that the Executive branch implement non-FISA electronic surveillance of persons in the United States and U.S. persons abroad with standards analogous to those in FISA whenever practicable, and that agency Inspectors General and General Counsels monitor compliance with dissemination procedures for such non-FISA surveillances in appropriate consultation with the Justice Department's Office of Intelligence Policy and Review. The Committee is requesting that future semiannual FISA reports of the Attorney General be accompanied by similar written reports on comparable non-FISA surveillances.

The Committee also believes that it might be worthwhile to consider the development of legislation to deal with the "state secrets privilege" in the context of lawsuits alleging violations of constitutional rights by non-FISA electronic surveillance or other techniques. Such legislation might reasonably be considered in conjunction with efforts to alleviate problems associated with the personal liability of federal officials.

Although the Act itself is sound, the Committee has found that aspects of the implementation and oversight of FISA surveillance raise a few concerns. The Committee has made classified recommendations in this regard to the Executive branch.

One recommendation with respect to FBI surveillance concerns terrorism cases in which the FBI appears to be more concerned with domestic law enforcement than with foreign intelligence collection. The courts are divided on whether the primary objective of a FISA surveillance must be to obtain foreign intelligence information, and the determination of purpose is left largely to the Executive branch. FISA surveillance in counterintelligence investigations and in international terrorism cases targeting terrorists who operate primarily abroad or on behalf of a foreign government will almost always be primarily to obtain foreign intelligence information. If, however, it is clear that the principal concern with respect to a terrorist group is domestic law enforcement and criminal prosecution, the FBI should use the law enforcement procedures under Title III of the Omnibus Crime Control Act of 1968 instead of FISA.

Regarding the overall administration of the Act, the Committee recommends that the three agencies most involved—the FBI, NSA, and the Office of Intelligence Policy and Review in the Justice Department—take measures to maintain continuity and experience in the personnel who review FISA surveillance requests and monitor compliance with minimization procedures. The quality of the officials who perform these duties is the single most important factor in the proper implementation of the Act.

The Committee has been asked by the American Civil Liberties Union to consider making public the number of U.S. persons who have been FISA surveillance targets. The Committee does not believe that the benefits of such disclosure for public understanding of FISA's impact would outweigh the damage to FBI foreign counterintelligence capabilities that can reasonably be expected to result. Any specific or approximate figure would provide significant information about the extent of the FBI's knowledge of the existence of hostile foreign intelligence agents in this country. As in other areas of intelligence oversight, the Committee must attempt to strike a proper balance between the need for public accountability and the secrecy required for effective intelligence operations.

Finally, the Committee has considered its own oversight procedures and the desirability of continuing to submit reports to the Senate on FISA implementation. The Act requires such reports only for the first five years. However, in view of the secrecy of FISA procedures and the importance of the constitutional rights and privacy concerns at stake, the Committee intends to continue to submit regular reports to the Senate at least every two years on the results of its oversight of FISA surveillance and related techniques that raise Fourth Amendment issues.

In conducting regular oversight of FISA implementation and related activities, the Committee will look closely at compliance with procedures designed to minimize the acquisition and prohibit the retention and dissemination of information about U.S. persons that is not clearly necessary for legitimate foreign intelligence and counterintelligence purposes. Such oversight is conducted primarily by the Justice Department's Office of Intelligence Policy and Review, and has not been undertaken by the Foreign Intelligence Surveillance Court despite its statutory authority to do so. The Committee will review all OIPR reports on the results of that office's minimization oversight and some surveillance logs, to assure itself that minimization procedures are being implemented properly. As a first step, the Committee is requesting that the Department of Justice provide it with copies of all past OIPR reports on such oversight and those surveillance logs that have been provided to courts or to other bodies outside the Executive branch.

The Committee has found it very useful to examine actual applications for FISA Court orders. It intends to increase this mode of oversight.

The Committee considers its oversight role to be an integral part of the system of checks and balances that is necessary to protect constitutional rights. The combination of Executive branch accountability, prior judicial review, and subsequent congressional scrutiny reflects the constitutional principle "that individual freedoms will best be preserved through a separation of powers and division of functions and levels of Government." [21]

[21] *United States* v. *United States District Court*, 407 U.S. 297, 318.

APPENDIX

Constitutional Status of Warrantless Physical Searches for Foreign Intelligence Purposes [22]

The constitutional problems with warrantless physical searches for foreign intelligence purposes are generally the same as those raised by warrantless electronic surveillance before the enactment of FISA.

The Supreme Court has never directly addressed either issue in the context of surveillance or search directed against foreign powers or foreign agents. However, in a 1972 decision holding unconstitutional the so-called "Mitchell doctrine" for warrantless electronic surveillance in domestic security cases, the Supreme Court recognized, in an opinion by Justice Powell, the need for "sensitivity both to the Government's right to protect itself from unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion." The Court explained the Fourth Amendment issues raised by warrantless surveillance:

> The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the law, to investigate, and to prosecute. But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.
>
> * * * * * * *
>
> The Fourth Amendment contemplates prior judicial judgment, not the risk that executive discretion may be reasonably exercised. This judicial role accords with our constitutional doctrine that individual freedoms will best be preserved through a separation of powers and division of functions and levels of Government. The independent check upon executive discretion is not satisfied . . . by "extremely limited" post-surveillance judicial review. Indeed, post-surveillance review would never reach the surveillance which failed to result in prosecution. Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights.

[22] This analysis was prepared by professional staff members for the Subcommittee on Legislation and the Rights of Americans.

Justice Powell then posited a two-part test to determine the balance between government and citizen interest:

> If the legitimate need of Government to safeguard domestic security requires the use of electronic surveillance, the question is whether the needs of citizens for privacy and free expression may not be better protected by requiring a warrant before such surveillance is undertaken. We must also ask whether a warrant requirement would unduly frustrate the efforts of Government to protect itself from acts of subversion and overthrow directed against it.[23]

Based on this test, the Court concluded that the President must obtain a warrant prior to conducting electronic surveillance in domestic security cases. The Court's ruling did not reach either surveillance of foreign powers and their agents or physical searches of any sort, but its description of a possible court order procedure for domestic security electronic surveillance influenced greatly the content of the eventual FISA legislation. The legislation was also influenced by a plurality of the Court of Appeals for the D.C. Circuit, which suggested in dictum that there should be no exception to the warrant requirement even for presidentially authorized foreign intelligence surveillance.[24] The other Federal courts that have addresed the question have sustained the Government's argument that there is an exception to the warrant requirement for electronic surveillance of foreign powers and foreign agents. All but one of these cases antedate passage of FISA;[25] that one, the *Truong-Humphrey* case, will be discussed presently because it also dealt with physical search.

The Federal courts have considered only two cases involving intelligence searches. In the *Ehrlichman* case arising from the search of Daniel Ellsberg's psychiatrist's office by the White House "plumbers" unit, the District Court's opinion stated that "the Government must comply with the strict constitutional and statutory limitations on trespassory searches and arrests even when known foreign agents are involved."[26] While the Court of Appeals in 1976 found it unnecessary to rule on this issue, because neither Ellsberg nor his psychiatrist was a foreign agent, two of the three judges filed a concurring opinion which declared that "physical entry into the home was the 'chief evil' appreciated by the framers of the Constitution"—a point that had also been made in the *Keith* case—and that national security electronic surveillance precedents may not apply to such intrusive searches.[27]

The Justice Department's analysis emphasizes the second case, which involved both warrantless electronic surveillance and the warrantless opening of three packages transmitted by a Vietnamese intelligence officer to an FBI asset for delivery abroad. In *Truong-Humphrey*, the District Court and the Court of Appeals for the Fourth Circuit dis-

[23] *United States* v. *United States District Court* (the "Keith" case), 407 U.S. 287, 303, 306 (1972).
[24] *Zweibon* v. *Mitchell*, 516 F.2d 594 (D.C. Cir. 1975), cert. denied, 425 U.S. 944 (1976).
[25] See *United States* v. *Brown*, 317 F. Supp. 531 (E.D.La. 1970), aff'd, 404 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974); *United States* v. *Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc), *cert. denied sub com. Ivanov* v. *United States*, 419 U.S. 881 (1974); *United States* v. *Buck*, 548 F.2d 871 (9th Cir. 1977), *cert. denied*, 434 U.S. 890 (1977).
[26] *United States* v. *Ehrlichman*, 376 F. Supp. 29, 33 (D.D.D. 1974).
[27] *United States* v. *Ehrlichman*, 546 F.2d 910 (D.C. Cir. 1976), opinion of Judge Leventhal.

posed of the search issue summarily in opinions that dealt almost entirely with warrantless electronic surveillance. The District Court noted:

> The Court is unpersuaded that there is any constitutional significance to the fact that this was a physical seizure and search and not an electronic search. It would be incongruous indeed were a court to find the opening of an envelope more instrusive than a wiretap or bug that runs for weeks at a time.[28]

The Court of Appeals did not discuss the relative instrusiveness of the different techniques and simply applied its warrantless electronic surveillance ruling to the searches.[29] It accepted the pre-*Keith* rationale that the President's constitutional powers for the conduct of foreign policy give him "the principal responsibility . . . for foreign intelligence surveillance" and took into account, following *Keith*, the practical difficulties that would "unduly frustrate" the President in attempting to get a warrant for each surveillance under normal procedures. All these cases occurred, of course, before FISA provided a court order procedure that would meet the Executive branch's needs for security, speed, and (over time) a measure of judicial expertise in the area of electronic surveillance.

Based on the *Truong-Humphrey* precedent and its own analysis of the constitutional issues, the Justice Department argues that no distinction should be made between electronic surveillance and other types of searches, or between trespassory and non-trespassory searches. Thus, the Justice Department believes that *Truong-Humphrey* reasoning is equally applicable to trespassory searches of private dwellings. The Supreme Court's refusal to consider the *Truong-Humphrey* appeal in 1982 leaves the Executive branch without definitive judicial guidance on these issues.

[28] *United States* v. *Humphrey*, 456 F. Supp. 51, 63 n. 13 (E.D.Va 1978).
[29] *United States* v. *Truong*, 629 F.2d 908, 917 n. 8 (4th Cir. 1980), *cert. denied*, 454 U.S. 1144 (1982).

○

END