

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

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

JUNE 8, 1978.—Ordered to be printed

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

REPORT

together with

SUPPLEMENTAL, ADDITIONAL, AND DISSENTING VIEWS

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

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

AMENDMENTS

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

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

TABLE OF CONTENTS

TITLE I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

- Sec. 101. Definitions.
- Sec. 102. Authorization for electronic surveillance for foreign intelligence purposes.
- Sec. 103. Special courts.
- Sec. 104. Application for an order.
- Sec. 105. Issuance of an order.
- Sec. 106. Use of information.
- Sec. 107. Report of electronic surveillance.
- Sec. 108. Congressional oversight.
- Sec. 109. Penalties.
- Sec. 110. Civil liability.

TITLE II—CONFORMING AMENDMENTS

- Sec. 201. Amendments to chapter 119 of title 18, United States Code.

TITLE III—EFFECTIVE DATE

- Sec. 301. Effective date.

(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if—

(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and

(C) any information acquired by such surveillance is used only to enforce chapter 119 of title 18, United States Code, or section 605 of the Communications Act of 1934, or to protect information from unauthorized surveillance; or

(3) train intelligence personnel in the use of electronic surveillance equipment, if—

(A) it is not reasonable to—

(i) obtain the consent of the persons incidentally subjected to the surveillance;

(ii) train persons in the course of surveillance otherwise authorized by this title; or

(iii) train persons in the use of such equipment without engaging in electronic surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

(C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

(g) Certifications made by the Attorney General pursuant to section 102(a) and applications made and orders granted under this title shall be retained in accordance with the security procedures established pursuant to section 103 for a period of at least ten years from the date of the application.

USE OF INFORMATION

Sec. 106. (a) Information acquired from an electronic surveillance conducted pursuant to this title concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this title. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this title shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this title may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) No information acquired pursuant to this title shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e) and the Government concedes that information obtained or derived from an electronic surveillance pursuant to the authority of this title as to which the moving party is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding, the Government may make a motion before the Special Court to determine the lawfulness of the electronic surveillance. Unless all the judges of the Special Court are so disqualified, the motion may not be heard by a judge who granted or denied an order or extension involving the surveillance at issue. Such motion shall stay any action in any court or authority to determine the lawfulness of the surveillance. In determining the lawfulness of the surveillance, the Special Court shall, notwithstanding any other law, if the Attorney General files an affidavit under oath with the Special Court that disclosure would harm the national security of the United States or compromise foreign intelligence sources and methods, review in camera the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the Special Court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials if there is a reasonable question as to the legality of the surveillance and if disclosure would likely promote a more accurate determination of such legality, or if such disclosure would not harm the national security.

(g) Except as provided in subsection (f), whenever any motion or request is made pursuant to any statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to surveillance pursuant to the authority of this title or to discover, obtain, or suppress any information obtained from electronic surveillance pursuant to the authority of this title, and the court or other authority determines that the moving party is an aggrieved person, if the Attorney General files with the Special Court of Appeals an affidavit under oath that an adversary hearing would harm the national security or compromise foreign intelligence sources and methods and that no information obtained from electronic surveillance pursuant to the authority of this title, and this title has been or is about to be used by the Government in the case before the court or other authority, the Special Court of Appeals shall, notwithstanding any other law, stay the proceeding before the other court or authority and review in camera and ex parte the application, order, and such other materials as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, and the Special Court of Appeals still disclose, under appropriate security procedures and protective orders, to the aggrieved person or his attorney portions of the application, order, or other materials relating to the surveillance only if necessary to afford due process to the aggrieved person.

(h) If the Special Court pursuant to subsection (f) or the Special Court of Appeals pursuant to subsection (g) determines the surveillance was not lawfully authorized and conducted, it shall, in accordance with the requirements of the law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the Special Court pursuant to subsection (f) or the Special Court of Appeals pursuant to subsection (g) determines the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(i) Orders granting or denying motions or requests under subsection (h), decisions under this section as to the lawfulness of electronic surveillance, and, absent a finding of unlawfulness, orders of the Special Court or Special Court of Appeals granting or denying disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except the Special Court of Appeals and the Supreme Court.

(j) In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any 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, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents may indicate a threat of death or serious bodily harm to any person.

(k) If an emergency employment of electronic surveillance is authorized under section 105(e) and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice, of—

- (1) the fact of the application;
- (2) the period of the surveillance; and
- (3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

REPORT OF ELECTRONIC SURVEILLANCE

SEC. 107. In April of each year, the Attorney General shall transmit to the Administrative Office of the United States Courts and to Congress a report setting forth with respect to the preceding calendar year—

- (a) the total number of applications made for orders and extensions of orders approving electronic surveillance under this title; and
- (b) the total number of such orders and extensions either granted, modified, or denied.

CONGRESSIONAL OVERSIGHT

SEC. 108. On a semiannual basis the Attorney General shall fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence concerning all electronic surveillance under this title. Nothing in this title shall be deemed to limit the authority and responsibility of those committees to obtain such additional information as they may need to carry out their respective functions and duties.

PENALTIES

SEC. 109. (a) OFFENSE.—A person is guilty of an offense if he intentionally—

- (1) engages in electronic surveillance under color of law except as authorized by statute; or
- (2) violates section 102(a)(2), 105(e), 105(f), 105(g), 106(a), 106(b), or 106(j) or any court order issued pursuant to this title, knowing his conduct violates an order or this title.

(b) DEFENSE.—(1) It is a defense to a prosecution under subsection (a)(1) that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

(2) It is a defense to a prosecution under subsection (a)(2) that the defendant acted in good faith belief that his actions did not violate any provisions of this title or any court order issued pursuant to this title, under circumstances where that belief was reasonable.

(c) PENALTY.—An offense described in this section is punishable by a fine of not more than \$10,000 or imprisonment for not more than five years, or both.

restriction, but the problems and circumstances of overseas surveillance demand separate treatment, and this bill, dealing with the area where most abuses have occurred, should not be delayed pending the development of that separate legislation. The committee notes the administration's commitment to the development of a separate bill governing overseas surveillances and expects to work closely with the administration on that bill.

SECTION-BY-SECTION ANALYSIS

Title I of the Foreign Intelligence Surveillance Act contains the substantive provisions governing the conduct of electronic surveillance for foreign intelligence purposes. Title II of the act contains certain amendments to chapter 119 of title 18, United States Code, governing the interception of wire and oral communications for law enforcement purposes, title III of the act contains the effective date and implementing provisions of the act.

As introduced, H.R. 7308 would have amended title 18 (Crimes and Criminal Procedure), United States Code, by creating a new chapter following chapter 119 which deals with law enforcement electronic surveillance. In the committee's view, the placement of title I in title 18 would be misleading. Nothing in title I relates to law enforcement procedures, and the one provision creating a criminal offense for intentional violations of the other provisions is pendent to the other provisions. Placing title I in title 18 would wrongly suggest either that the bill's procedures deal with law enforcement or that the thrust of the bill is to create a Federal crime. Because the bill instead establishes authorities and procedures dealing with the collection of foreign intelligence, the committee believes that its proper placement would be in title 50 (War and National Defense), United States Code. Title 50 has traditionally been the title in which laws relating to this Nation's intelligence activities have been placed, for example, the National Security Act of 1947 and the CIA Act of 1949.

This change from the bill as introduced, however, is not intended to affect in any way the jurisdiction of congressional committees with respect to electronic surveillance for foreign intelligence purposes. Rather, the purpose of the change is solely to allow the placement of title I in that portion of the United States Code which most directly relates to its subject matter.

Section 101

This section contains all the definitions of terms used in the bill. Because most of the substantive aspects of the bill derive from the definition of particular terms, this section is critical to the bill as a whole.

(a) "*Foreign power*"

Subsection (a) defines "foreign power" in six separate ways. These definitions are crucial because surveillances may only be targeted against foreign powers or agents of foreign powers.

It is expected that certain of the defined "foreign powers" will be found in the United States and targeted directly; others are not likely to be found in the United States but are included in the definition more to enable certain persons who are their agents, and who may be in the United States, to be targeted as "agents of a foreign power,"

in West Berlin) are not under the territorial sovereignty of the United States.

In the bill terms such as "foreign-based" and "foreign territory" refer to places outside the "United States," as defined here.

(k) Aggrieved person

Section 101(k) defines the term "aggrieved person" as a person who has been the target of an electronic surveillance or any other person who, although not a target, has been incidentally subjected to electronic surveillance. As defined, the term is intended to be coextensive, but no broader than, those persons who have standing to raise claims under the Fourth Amendment with respect to electronic surveillance. See *Alderman v. United States*, 394 U.S. 316 (1968).

The term specifically does not include persons, not parties to a communication, who may be mentioned or talked about by others. The Supreme Court has specifically held in *Alderman* that such persons have no fourth amendment privacy right in communications about them which the Government may intercept. While under this bill minimization procedures require minimization of communications about U.S. persons, even though they are not parties to the communication, there is no intent to create a statutory right in such persons which they may enforce. Suppression of relevant criminal evidence and civil suit are particularly inappropriate tools to insure compliance with this part of minimization. Review by judges pursuant to section 105(d), Executive oversight and congressional oversight by the Senate and House Intelligence Committees are intended to be the exclusive means by which compliance with minimization procedures governing minimization of "mentions of" U.S. persons is to be monitored under this or any other law.

(1) Wire communication

Section 101(1) defines "wire communication" to mean any communication (whether oral, verbal, or otherwise) while it is being carried by a wire, cable, or other like connection furnished or operated by a communications common carrier. This definition of wire communication differs from the definition of the same term in chapter 119 of title 18, United States Code. There the term is defined to include any communication carried in whole or in part by a wire furnished by a common carrier. This has led to anomalous results such as where a woman listening to an ordinary FM radio has intercepted radio-telephone communications and thereby technically violated chapter 119. See *United States v. Hall*, 488 F. 2d 193 (9th Cir. 1973). Also, ordinary marine band communications, which do not have a reasonable expectation of privacy or require a warrant for law enforcement interception, can be "patched into" telephone systems, becoming a "wire communication" under chapter 119.

The definition here makes clear that communications are "wire communications" under the bill only while they are carried by a wire furnished or operated by a common carrier. The term "common carrier" means a U.S. common carrier and not a common carrier in a foreign country. Moreover, the word "furnished" means furnished in the ordinary course of the common carrier's provision of communications facilities. It does not refer to equipment sold outright to a

person. The effect of this is to require a tap on the wire, an induction coil or like device to acquire the communication from the wire furnished by the common carrier for the activity to be electronic surveillance under section 101 (f) (2). Interception of microwave communications carried by common carriers, by intercepting the radio signal, is electronic surveillance under section 101 (f) (3), not section 101 (f) (2), involving acquisition of a radio communication, not a wire communication. A radio signal is not within the term, a "like connection," in this definition.

(m) Person

Section 101 (m) defines "person" in the broadest sense possible. It is intended to make explicit that entities can be persons, where the term "person" is used. For example, while it is expected that most entities would be targeted under the "foreign power" standard (which cannot be applied to individuals), it is possible that entities could be targeted under certain of the "agent of a foreign power" standards, see section 101 (b) (2) (A)-(D). Where it is intended that only natural persons are referred to, the term "individual" U.S. person or "individual" person is used.

(n) Contents

Section 101 (n) defines the term "contents", when used with respect to any communication, in broad terms. Specifically, it includes any information concerning the identities of the parties or the existence, substance, purport, or meaning of a communication. This broad phrasing is meant to assure that the scope of the bill is sufficient to protect legitimate privacy interests. Inasmuch as three of the four subdefinitions of electronic surveillance, which in fact define the coverage of the bill, turn on the acquisition of "contents" it is necessary to assure that devices such as pen registers are included.

In a recent decision,²² the Supreme Court suggested that a pen register did not acquire "contents" of a "wire communication" as those terms are defined in chapter 119 of title 18, United States Code.²³ It is the intent of this committee that pen registers do acquire "contents" of "wire communications" as those terms are defined in this bill. The term "contents" specifically mentions the identity of parties and "identity" includes a person's phone number, which can as effectively identify him as the mention of his name. Moreover, the definition of "contents" includes information concerning the "existence" of a communication. When a person dials another person's telephone number, whether or not the other person answers the phone, this is a communication under this bill. This is especially true in the intelligence field where signals to a spy may be conveyed merely by having the phone ring a designated number of times. The fact that the target of the pen registers has attempted to communicate with another person at a particular phone is information concerning the "existence" of the communication.

Of course, acquiring knowledge of the "existence" of communications in general, as opposed to acquiring knowledge of the "existence" of a particular communication or communications is not within the

²² *United States v. N.Y. Telephone Co.*, — U.S. — (1977).

²³ This aspect of the decision seems gratuitous because the Court noted that pen registers do not result in the "aural acquisition" of anything, which would be required, to bring them under chapter 119.

The committee also recognizes that training in laboratory conditions may not be sufficient; field training in almost all areas of endeavor is considered necessary. Finally, communications acquired in the course of training personnel are barred from being retained or disseminated. There is no need for anyone other than the trainees and their instructor to have any knowledge of what might or might not have been intercepted.

The authorization in this subsection is a narrow one made necessary by the broad definition of "electronic surveillance." It is not intended to authorize electronic surveillances to gather foreign intelligence information generally. Thus the provision is phrased in terms of the purpose being "solely to test the capability of electronic equipment . . . , determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance . . . or training intelligence personnel in the use of electronic surveillance equipment." Where, for example, the existence and capability of unauthorized electronic surveillance equipment has been established, this provision does not authorize further surveillance to determine the targets of the surveillance or the information being acquired by the unauthorized surveillance.

All tests, "sweeps" and training conducted pursuant to this provision must be in the normal course of official business by the Government agent conducting the test, sweep, or training. The committee contemplates that such testing, "sweeps," and training will be approved by a senior official prior to the commencement of the activity.

Subsection (g) was not in H.R. 7308, as introduced. Its effect is self-explanatory. Its purpose is to assure accountability by requiring that applications and orders be maintained for 10 years. Under chapter 119 of title 18, U.S.C., there is a similar 10 year recordkeeping requirement.

Section 106

This section places additional constraints on Government use of information obtained from electronic surveillance and establishes detailed procedures under which such information may be received in evidence, suppressed, or discovered.

Subsection (a) requires that information concerning U.S. persons acquired from electronic surveillance pursuant to this title may be used and disclosed by Federal officers and employees, without the consent of the U.S. person, only in accordance with the minimization procedures defined in section 101(h). This provision ensures that the use of such information is carefully restricted to actual foreign intelligence or law enforcement purposes.

This subsection also notes that no otherwise privileged communication obtained in accordance with or in violation of this chapter shall lose its privileged character. This provision is identical to 18 U.S.C. 2517(4) and is designed, like its title III predecessor, to change existing law as to the scope and existence of privileged communications only to the extent that it provides that otherwise privileged communications do not lose their privileged character because they are intercepted by a person not a party to the conversation.

Subsection (a) further states that no information (whether or not it concerns a U.S. person) acquired from an electronic surveillance

pursuant to this title may be used or disclosed except for lawful purposes. This provision did not appear in H.R. 7308, as introduced. It was added by the committee to insure that information concerning foreign visitors and other non-U.S. persons, the use of which is not restricted to foreign intelligence or law enforcement purposes, is not used for illegal purposes.

There is no specific restriction in the bill regarding to whom Federal officers may disclose information concerning U.S. persons acquired pursuant to this title although specific minimization procedures might require specific restrictions in particular cases. First, the committee believes that dissemination should be permitted to State and local law enforcement officials. If Federal agents monitoring a foreign intelligence surveillance authorized under this title were to overhear information relating to a violation of State criminal law, such as homicide, the agents could hardly be expected to conceal such information from the appropriate local officials. Second, the committee can conceive of situations where disclosure should be made outside of Government channels. For example, Federal agents may learn of a terrorist plot to kidnap a business executive. Certainly in such cases they should be permitted to disclose such information to the executive and his company in order to provide for the executive's security.

Finally, the committee believes that foreign intelligence information relating to crimes, espionage activities, or the acts and intentions of foreign powers may, in some circumstances, be appropriately disseminated to cooperating intelligence services of other nations. So long as all the procedures of this title are followed by the Federal officers, including minimization and the limitations on dissemination, this cooperative relationship should not be terminated by a blanket prohibition on dissemination to foreign intelligence services. The committee wishes to stress, however, that any such dissemination be reviewed carefully to ensure that there is a sufficient reason why disclosure of information to foreign intelligence services is in the interests of the United States.

Disclosure, in compelling circumstances, to local officials for the purpose of enforcing the criminal law, to the targets of clandestine intelligence activity or planned violence, and to foreign intelligence services under the circumstances described above are generally the only exceptions to the rule that dissemination should be limited to Federal officials.

It is recognized that these strict requirements only apply to information known to concern U.S. persons. Where the information in the communication is encoded or otherwise not known to concern U.S. persons, only the requirement that the information be disclosed for lawful purposes applies. There is no requirement that before disclosure can be made information be decoded or otherwise processed to determine whether information concerning U.S. persons is indeed present. Of course, the restrictions on use and disclosure still apply, so that if any Government agency received coded information from the intercepting agency, were it to break the code, the limitations on use and disclosure would apply to it.

Subsection (b) requires that disclosure of information for law enforcement purposes must be accompanied by a statement that such

evidence, or any information derived therefrom, may be used in a criminal proceeding only with the advance authorization of the Attorney General. This provision is designed to eliminate circumstances in which a local prosecutor has no knowledge that evidence was obtained through foreign intelligence electronic surveillance. In granting approval of the use of evidence the Attorney General would alert the prosecutor to the surveillance and he, in turn, could alert the court in accordance with subsection (c) or (d).

Subsections (c) through (i) set forth the procedures under which information acquired by means of electronic surveillance may be received in evidence or otherwise used or disclosed in any trial, hearing or other Federal or State proceeding. Although the primary purpose of electronic surveillance conducted pursuant to this chapter is not likely to be the gathering of criminal evidence, it is contemplated that such evidence will be acquired and these subsections establish the procedural mechanisms by which such information may be used in formal proceedings.

At the outset the committee recognizes that nothing in these subsections abrogates the rights afforded a criminal defendant under *Brady v. Maryland*,⁴³ and the Jencks Act.⁴⁴ These legal principles inhere in any such proceeding and are wholly consistent with the procedures detailed here. Furthermore, nothing contained in this section is intended to alter the traditional principle that the Government cannot use material at trial against a criminal defendant, and then withhold from him such material at trial.⁴⁵

Subsection (c) states that no information acquired from an electronic surveillance (or any fruits thereof) may be used against an aggrieved person, as defined, unless prior to the trial, hearing, or other proceeding, or at a reasonable time prior to an effort to disclose the information or submit it in evidence, the United States notifies the court or other authority and the aggrieved person of its intent.

Subsection (d) places the same requirements upon the states and their political subdivisions, and also requires notice to the Attorney General.

Subsection (e) provides a separate statutory vehicle by which an aggrieved person against whom evidence derived or obtained from an electronic surveillance is to be or has been introduced or otherwise used or disclosed in any trial, hearing or proceeding may move to suppress the information acquired by electronic surveillance or evidence derived therefrom. The grounds for such a motion would be that (1) the information was unlawfully acquired, or (2) the surveillance was not made in conformity with the order of authorization or approval.

A motion under this subsection must be made before the trial, hearing, or proceeding unless there was no opportunity to make such a motion or the movant was not aware of the grounds for the motion.

It should be noted that the term "aggrieved person", as defined in section 101(k) does not include those who are mentioned in an intercepted communication. The committee wishes to make it clear that

⁴³ 373 U.S. 83 (1963).

⁴⁴ 18 U.S.C. 3500 et seq.

⁴⁵ *United States v. Andolschek*, 142 F.2d 503 (2nd Cir. 1944)

such persons do not have standing to file a motion under section 106 or under any other provision. The minimization procedures do apply to such persons and, to the extent that such persons lack standing, the committee recognizes that it has created a right without a remedy. However, it is felt that the Attorney General's regulations concerning the minimization procedures, judicial review of such procedures, and criminal penalties for intentional violation of them, will provide sufficient protection.

Section (f) sets out special judicial procedures to be followed when the Government concedes that it intends to use or has used evidence obtained or derived from electronic surveillance. Where, in any trial or proceeding, the Government concedes, either pursuant to the notification⁴⁶ requirements of subsection (c) and (d) or after a motion is filed by the defendant pursuant to subsection (e), that it intends to use or has used evidence obtained or derived from electronic surveillance, it may make a motion before the special court to determine the lawfulness of the surveillance. The special court must then determine whether the surveillance was lawful or not. In so doing, no judge who granted an order or extension involving the surveillance at issue could make the determination, unless all the judges of the special court would be so disqualified.

The determination would be made in camera if the Attorney General certifies under oath that disclosure would harm the national security or compromise foreign intelligence sources and methods.⁴⁷ However, when the special court determines that there is a reasonable question as to the legality of the surveillance and disclosure would likely promote a more accurate determination thereof (or when the court determines that disclosure would not harm the national security) the defendant should be provided relevant portions of the application, order, or other materials. Whenever there is a reasonable question of legality, it is hoped that disclosure, with an in camera adversary hearing, will be the usual practice. The committee considered requiring an adversary hearing in all cases, but was persuaded by the Department of Justice that in those instances where there is no reasonable question as to the legality of the surveillance security considerations should prevail. In ordering disclosure, the special court must provide for appropriate security procedures and protective orders.

Subsection (f), outlined above, deals with those rare situations in which the Government states it will use evidence obtained or derived from an electronic surveillance.

Subsection (g) states in detail the procedures to be followed when, in any court or other authority of the United States or a state, a motion or request is made to discover or obtain applications or orders, or other materials relating to surveillance under this title, or to dis-

⁴⁶ It should be emphasized that notification by the Government triggers the special court procedures whether or not the defense has filed a suppression or discovery motion. Thus, if, before the filing of such motions, the Government concedes use of evidence obtained from electronic surveillance, and the Court determines that the surveillance was lawful, a discovery or suppression motion would be moot because of the requirements of subsection (h).

⁴⁷ In many, if not most cases, the Attorney General's affidavit will have to be based on information supplied to him by other Executive officers. It is perfectly proper for the Attorney General in making his affidavit to rely on conclusions and beliefs held by others in the Executive Branch who are responsible for national security or intelligence sources and methods.

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

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

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

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

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

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

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

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

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

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

considerations, it is believed, suggest that—given the in camera procedure—the private party will be more thoroughly protected by having the special courts determine the legality of the surveillances under the bill.

The most significant change is contained in the subsection (f) provision authorizing disclosure and an adversary hearing in certain circumstances. This provision has been adopted only after lengthy discussion within the committee and a careful consideration of the suggested risk to security involved. The narrow reach of the provision should be emphasized: the adversary hearing procedures can arise only in those instances where the Government concedes that it intends to use evidence obtained or derived from an electronic surveillance (which the Government had not done in the last 10 years until the case of *U.S. v. Humphrey*, crim. no. 78-25-A, E.D. Va.).

Furthermore, the decision to remove a proceeding to one of the special courts (under subsection (f) or (g)), is entirely up to the Government in the first instance, as, of course, is the decision to prosecute. With these limitations, the committee believes that the adversary hearing provision is fully protective of those legitimate security interests which the Congress, no less than the executive branch, has a duty to safeguard.

The Congress has an equally compelling duty to insure that trials are conducted according to traditional American concepts of fair play and substantial justice. In this context, the committee believes that when the Government intends to use information against a criminal defendant obtained or derived from an electronic surveillance, and there is a reasonable question as to the legality of a surveillance, simple justice dictates that the defendant not be denied the use of our traditional means for reaching the truth—the adversary process.⁴⁹

Where the Government states under oath that it does not intend to use evidence or information obtained or derived from electronic surveillance, the case for an adversary hearing is less persuasive and the bill does not provide for it. In such cases, however, in order to provide additional protection to the defendant, the bill (if the case is removed from the trial court) states that the matter be heard by three judges of the special court of appeals, rather than by a single judge of the special court.

It should be emphasized that in determining the legality of a surveillance under subsection (f) or (g), the judges of the special courts (or the trial judge if the matter is not removed to the special courts) are not to make determinations which the issuing judge is not authorized to make. Where the bill specifies the scope or nature of judicial review in the consideration of an application, any review under these subsections is similarly constrained. For example, when reviewing the certifications required by section 104(a)(7), unless there is a prima facie

⁴⁹ The committee is aware that the Supreme Court has never decided that an adversary hearing is constitutionally required to determine the legality of a surveillance. See *Alderman v. United States*, 394 U.S. 165 (1968); *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc), cert. denied sub nom. *Ivanov v. United States*, 419 U.S. 881 (1974); *Giordano v. United States*, 394 U.S. 310, 314 (1968) (concurring opinion of Justice Stewart.) This fact does not lessen the importance of an adversary hearing in searching for the truth and assuring a fair trial, and if the court should so decide, the procedures for an adversary hearing would already be in place. It should also be noted that in neither *Alderman* nor *Butenko* did the Government concede use of information obtained or derived from a surveillance.

showing of a fraudulent statement by a certifying officer, procedural regularity is the only determination to be made if a non-U.S. person is the target, and the "clearly erroneous" standard is to be used where a U.S. person is targeted. Of course, the judge is also free to review the constitutionality of the law itself.

Subsection (h) states what procedures the special courts are to follow after a determination of legality or illegality is made pursuant to subsection (f) or (g). The committee wishes to emphasize that its intent in this provision is not to legislate new procedures or in any other manner alter existing procedures with respect to what should be ordered after a finding of illegality is made. In such circumstances, the judge is directed to suppress the evidence or otherwise grant the motion "in accordance with the requirements of law." Existing case law requires the Government, in the case of an illegal surveillance, to surrender to the defendant all the information illegally acquired in order for the defendant to make an intelligent motion on the question of taint. The Supreme Court in *Alderman v. United States*, *supra*, held that once a defendant claiming evidence against him was the fruit of unconstitutional electronic surveillance has established the illegality of such surveillance (and his "standing" to object), he must be given those materials illegally acquired in the Government's files to assist him in establishing the existence of "taint." The Court rejected the Government's contention that the trial court could be permitted to screen the files in camera and give the defendant only material which was "arguably relevant" to his claim, saying such screening would be sufficiently subject to error to interfere with the effectiveness of adversary litigation of the question of "taint." The Supreme Court has refused to reconsider the *Alderman* rule and, in fact reasserted its validity in its *Keith* decision. (*United States v. U.S. District Court*, *supra*, at 393).

As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

A decision of illegality may not always arise in the context of suppression; rather it may, for example, arise incident to a discovery motion in a civil trial. Here, again, the bill does not specify what the court should order. Again, the court should grant the motion only "in accordance with requirements of law." Here, however, the requirements of law would be those respecting civil discovery. In other words, once the surveillance is determined to be unlawful, the intent of this section is to leave to otherwise existing law the resolution of what, if anything, is to be disclosed. For instance, under the Freedom of Information Act, other defenses against disclosure may be able to be made.

Where the court determines pursuant to subsections (f) or (g) that the surveillance was lawfully authorized and conducted, it would, of course, deny any motion to suppress. In addition, once a judicial determination is made that the surveillance was lawful, any motion or request to discover or obtain materials relating to a surveillance must

be denied unless disclosure or discovery is required by due process.⁵

Subsection (i) states for purposes of appeal that orders or decisions of the special courts granting or denying motions, deciding the lawfulness of a surveillance or ordering or denying disclosure shall be final orders, and shall be binding upon all courts of the United States and the States except the special court of appeals and the Supreme Court. As final orders they will be immediately appealable, by the private party or the government. The committee recognizes that the usual practice is to consider such orders interlocutory and not immediately appealable.

In the particular circumstances of cases handled pursuant to subsections (c)–(i), however, the committee believes that substantial considerations militate in favor of immediate appeal. Requirements to disclose certain information, whether before or after a finding of illegality, might force the Government to dismiss the case (or concede the case, if it were a civil suit against it) to avoid disclosure it thought not required. This is not the situation in normal cases, and therefore it is appropriate here to allow immediate appeal of such an order. Similarly, given the in camera and to a greater or lesser extent ex parte proceedings under subsections (f) and (g), it is appropriate to afford a more expeditious form of appeal for the private litigant. Because cases under these subsections are not expected to occur often, there is no meaningful added burden placed on the courts by allowing such interlocutory orders.

New subsection (j) has been added to the bill for the purpose of restricting the use of unintentionally acquired private domestic radio communications. The new subsection is needed because “electronic surveillance” as defined in 101(f)(3) covers only the intentional acquisition of the contents of private domestic radio communications. Such communications may include telephone calls and other wire communications transmitted by radio microwaves. Concern has been expressed that unless the use of such unintentionally acquired communications is restricted, there would be a potential for abuse if the Government acquired those kinds of domestic communications, even without intentionally targeting any particular communication. The amendment forecloses this possibility by restricting the use of any information acquired in this manner.

In circumstances involving the unintentional acquisition, by an electronic, mechanical, or other surveillance device of the contents of any radio communication, where a persons has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and where both the sender and all intended recipients are located within the United States, the contents must be destroyed upon recognition. The only exception is with the approval of the Attorney General where the contents indicate a threat of death or serious bodily harm to any person. This restriction is not intended to prevent the Government from maintaining a record of the radio frequency of the communication for later collection avoidance purposes.

⁵⁰ The committee recognizes that this provision alters existing law and is a limitation on existing discovery practice. It is felt that where the special court has determined that the surveillance is lawful, security considerations should preclude any disclosure unless due process requires disclosure.

Subsection (k) provides for notice to be served on U.S. citizens and permanent resident aliens who were targets of an emergency surveillance and, in the judge's discretion, on other citizens and resident aliens who are incidentally overheard, where a judge denies an application for an order approving an emergency electronic surveillance. Such notice shall be limited to the fact that an application was made, the period of the emergency surveillance, and the fact that during the period information was or was not obtained. This notice may be postponed for a period of up to 90 days upon a showing of good cause to the judge. Thereafter the judge may forego the requirement of notice upon a second showing of good cause.

The fact which triggers the notice requirement—the failure to obtain approval of an emergency surveillance—need not be based on a determination by the court that the target is not an agent of a foreign power engaged in clandestine intelligence activities, sabotage, or terrorist activities or a person aiding such agent. Failure to secure a court order could be based on a number of other factors, such as an improper certification. A requirement of notice in all cases would have the potential of compromising the fact that the Government has focused an investigation on the target. Even where the target is not, in fact, an agent of a foreign power, giving notice to the person may result in compromising an ongoing foreign intelligence investigation because of the logical inferences a foreign intelligence service might draw from the targeting of the individual. For these reasons, the Government is given the opportunity to present its case to the judge for initially postponing notice. After 90 days, during which time the Government may be able to gather more facts, the Government may seek the elimination of the notice requirement altogether.

It is the intent of the committee that if the Government can initially show that there is a reason to believe that notice might compromise an ongoing investigation, or confidential sources or methods, notice should be postponed. Thereafter, if the Government can show a likelihood that notice would compromise an ongoing investigation, or confidential sources or methods, notice should not be given.

Section 107

Section 107 requires the submission of annual reports to both the Congress and the Administrative Office of the U.S. Courts containing statistical information relating to electronic surveillance under this title. The reports must include the total number of applications made for orders and extensions and the total number of orders or extensions granted, modified, and denied. The statistics in these reports should present a quantitative indication of the extent to which surveillance under this title is used. The committee intends that such statistics will be public.

Section 108

Congressional oversight is particularly important in monitoring the operation of this statute. By its very nature foreign intelligence surveillance must be conducted in secret. The bill reflects the need for such secrecy: judicial review is limited to a select panel and routine notice to the target is avoided. In addition, contrary to the premises which underlie the provisions of title III of the Omnibus Crime Con-

