Exhibit A
S. 1566

IN THE HOUSE OF REPRESENTATIVES

April 24, 1978

Referred to the Committee on the Judiciary

AN ACT

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.

1 Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

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

3 Sec. 2. Title 18, United States Code, is amended by

4 adding a new chapter after chapter 119 as follows:

5

6
"Chapter 120.—ELECTRONIC SURVEILLANCE WITH
IN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES"

"Sec. 2521. Definitions.
2523. Designation of judges authorized to grant orders for electronic surveillance.
2524. Application for an order.
2525. Issuance of an order.
2526. Use of information.
2528. Congressional oversight.

"§ 2521. Definitions

"(a) Except as otherwise provided in this section the definitions of section 2510 of this title shall apply to this chapter.

"(b) As used in this chapter—

"(1) 'Foreign power' means—

"(A) a foreign government or any component thereof, whether or not recognized by the United States;

"(B) a faction of a foreign nation or nations, not substantially composed of United States persons;

"(C) an entity, which is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
"(ii) the successful conduct of the foreign affairs of the United States; or

"(C) information which relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

"(i) sabotage or terrorism by a foreign power or an agent of a foreign power, or

"(ii) the clandestine intelligence activities of an intelligence service or network of a foreign power or an agent of a foreign power.

"(6) "Electronic surveillance" means—

"(A) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, where the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

"(B) the acquisition by an electronic, mechanical, or other surveillance device, of the contents of any wire communication to or from a person in the United States, without the consent of any party
thereto, where such acquisition occurs in the United States while the communication is being transmitted by wire;

"(C) the intentional 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 where both the sender and all intended recipients are located within the United States; or

"(D) the installation or use of an electronic, mechanical, or other 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.

"(7) 'Attorney General' means the Attorney General of the United States (or Acting Attorney General) or the Deputy Attorney General.

"(8) 'Minimization procedures' means procedures which are reasonably designed to minimize the acquisition and retention, and prohibit the dissemination, except as provided for in subsections 2526 (a) and (b), of
the surveillance, no information obtained or evidence
derived from such surveillance shall be received in
evidence or otherwise disclosed in any trial, hearing,
or other proceeding in or before any court, grand jury,
department, office, agency, regulatory body, legislative
committee, or other authority of the United States, a
State, or political subdivision thereof; and no informa-
tion concerning any United States person acquired from
such surveillance shall subsequently be used or dis-
closed in any other manner by Federal officers or
employees without the consent of such person, except
with the approval of the Attorney General where the
information indicates a threat of death or serious bodily
harm to any person. A denial of the application made
under this subsection may be reviewed as provided
in section 2523.

§ 2526. Use of information

(a) Information concerning United States persons
acquired from an electronic surveillance conducted pursuant
to this chapter may be used and disclosed by Federal officers
and employees without the consent of the United States per-
son only for purposes specified in section 2521 (b) (8) (A)
through (F) and in accordance with the minimization pro-
cedures required by this chapter, or for the enforcement of
the criminal law if its use outweighs the possible harm to
the national security. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character. No information acquired from an electronic surveillance conducted pursuant to this chapter may be used or disclosed by Federal officers or employees except for lawful purposes.

"(b) The minimization procedures required under this chapter shall not preclude the retention and disclosure, for law enforcement purposes, of any information which constitutes evidence of a crime if such disclosure is accompanied by a statement that such evidence, 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 of the United States, of a State, or of a 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, or other authority of the United States, a State, or a political subdivision thereof, any information obtained or derived from an electronic surveillance, 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 the information or submit it in evidence notify the court in which the information is to be disclosed or used or, if the information is to be disclosed or used in or
before another authority, shall notify a court in the district
wherein the information is to be so disclosed or so used that
the Government intends to so disclose or so use such infor-
mation.

"(d) Any person who has been the target of electronic
surveillance or whose communications or activities have been
subject to electronic surveillance and against whom evidence
derived from such electronic surveillance is to be, or has
been, introduced or otherwise used or disclosed in any trial,
hearing, or proceeding in or before any court, department
officer, agency, regulatory body or other authority of the
United States, a State, or a political subdivision thereof,
may move to suppress the contents of any communication
acquired by electronic surveillance, or evidence derived
therefrom, on the grounds that—

"(1) the communication was unlawfully acquired;
or

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

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

"(e) Whenever any court is notified in accordance with
subsection (c), or whenever a motion is made by an ag-
grieved person pursuant to subsection (d), to suppress evidence on the grounds that it was obtained or derived from an unlawful electronic surveillance, or whenever any motion or request is made by an aggrieved person pursuant to section 3504 of this title or any other statute or rule of the United States, to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance, the Federal court, or where the motion is made before another authority, a Federal court in the same district as the authority, shall, notwithstanding any other law, if the Government by affidavit asserts that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and other materials relating to the surveillance as may be necessary to determine whether the surveillance was authorized and conducted in a manner that did not violate any right afforded by the Constitution and statutes of the United States to the aggrieved person. In making this determination, the court shall disclose to the aggrieved person portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance. If the court determines that the electronic surveillance of the aggrieved person was not lawfully authorized or conducted, the court shall in accordance with the requirements of law suppress the
information obtained or evidence derived from the unlawful electronic surveillance. If the court determines that the surveillance was lawfully authorized and conducted, the court shall deny any motion for disclosure or discovery unless required by due process.

"(f) If an emergency employment of the electronic surveillance is authorized under section 2525(d) 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.

"(g) In circumstances involving the unintentional acquisition, by an electronic, mechanical, or other surveil-
lance 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 where both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, except with the approval of the Attorney General where the contents indicate a threat of death or serious bodily harm to any person.

§ 2527. Report of electronic surveillance

"In April of each year, the Attorney General shall report to the Administrative Office of the United States Courts and shall transmit to Congress with respect to the preceding calendar year—

"(1) the total number of applications made for orders and extensions of orders approving electronic surveillance; and

"(2) the total number of such orders and extensions either granted, modified, or denied.

§ 2528. Congressional oversight

"(a) 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 chapter. Nothing in this chapter shall be deemed to limit the author-
ity and responsibility of the appropriate committees of each House of Congress to obtain such additional information as they may need to carry out their respective functions and duties.

"(b) On or before one year after the effective date of this chapter, and on the same day each year thereafter, the Select Committee on Intelligence of the United States Senate shall report to the Senate, concerning the implementation of this chapter. Said reports shall include but not be limited to an analysis and recommendations concerning whether this chapter should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment."

Sec. 3. The provisions of this Act and the amendment made hereby shall become effective upon enactment: Provided, That any electronic surveillance approved by the Attorney General to gather foreign intelligence information shall not be deemed unlawful for failure to follow the procedures of chapter 120, title 18, United States Code, if that surveillance is terminated or an order approving that surveillance is obtained under this chapter within ninety days following the designation of the first judge pursuant to section 2523 of chapter 120, title 18, United States Code.

Sec. 4. Chapter 119 of title 18, United States Code, is amended as follows:

(a) Section 2511 (1) is amended—
(1) by inserting "or chapter 120 or with respect to
techniques used by law enforcement officers not involv-
ing the interception of wire or oral communications
as otherwise authorized by a search warrant or order of
a court of competent jurisdiction," immediately after
"chapter" in the first sentence;

(2) by inserting a comma and "or, under color of
law, willfully engages in any other form of electronic
surveillance as defined in chapter 120" immediately
before the semicolon in paragraph (a);

(3) by inserting "or information obtained under
color of law by any other form of electronic surveillance
as defined in chapter 120" immediately after "contents
of any wire or oral communication" in paragraph (c);

(4) by inserting "or any other form of electronic
surveillance, as defined in chapter 120," immediately
before "in violation" in paragraph (c);

(5) by inserting "or information obtained under
color of law by any other form of electronic surveillance
as defined in chapter 120" immediately after "any wire
or oral communication" in paragraph (d); and

(6) by inserting "or any other form of electronic
surveillance, as defined in chapter 120," immediately
before "in violation" in paragraph (d).

(b) (1) Section 2511 (2) (a) (i) is amended by insert-
(2) Section 2511 (2) (a) (ii) is amended by inserting the words “or chapter 120” after the second appearance of the word “chapter,” and by striking the period at the end thereof and adding the following: “or engage in electronic surveillance, as defined in chapter 120: Provided, however, that before the information, facilities, or technical assistance may be provided, the investigative or law enforcement officer shall furnish to the officer, employee, or agent of the carrier either—

“(1) an order signed by the authorizing judge certifying that a court order directing such assistance has been issued; or

“(2) in the case of an emergency interception or electronic surveillance as provided for in section 2518 (7) of this chapter or section 2525 (d) of chapter 120, a certification under oath by the investigative or law enforcement officer that the applicable statutory requirements have been met,

and setting forth the period of time for which the electronic surveillance is authorized and describing the facilities from which the communication is to be acquired. Any violation of this subsection by a communication common carrier or an
officer, employee, or agency thereof, shall render the carrier
liable for the civil damages provided for in section 2520. No
communication common carrier or officer, employee, or
agent thereof shall disclose the existence of any interception
under this chapter or electronic surveillance, as defined in
chapter 120, with respect to which the common carrier
has been furnished either an order or certification under
this subparagraph, except as may otherwise be lawfully
ordered.”.

(c) (1) Section 2511 (2) (b) is amended by inserting
the words “or otherwise engage in electronic surveillance, as
defined in chapter 120,” after the word “radio”.

(2) Section 2511 (2) (e) is amended by inserting the
words “or engage in electronic surveillance, as defined in
chapter 120,” after the words “oral communication” and by
inserting the words “or such surveillance” after the last word
in the paragraph and before the period.

(3) Section 2511 (2) is amended by adding at the end
of the section the following provisions:

“(e) Notwithstanding any other provision of this title
or section 605 or 606 of the Communications Act of 1934,
it shall not be unlawful for an officer, employee, or agent of
the United States in the normal course of his official duty
under procedures approved by the Attorney General to
conduct electronic surveillance as defined in section 2521
(b) (6) of chapter 120 without a court order for the sole
purpose of:

"(i) testing the capability of electronic equipment,
provided that no particular United States person shall
be intentionally targeted for testing purposes without
his consent, the test period shall be limited in extent
and duration to that necessary to determine the capabil-
ity of the equipment, that the content of any communica-
tion acquired under this paragraph shall be retained
and used only for the purpose of determining the ca-
pability of such equipment, shall be disclosed only to the
persons conducting the test, and shall be destroyed upon
completion of the testing, and that the test may exceed
ninety days only with the prior approval of the Attorney
General; or

"(ii) determining the existence and capability of
electronic surveillance equipment being used unlawfully,
provided that no particular United States person shall
be intentionally targeted for such purposes without his
consent, that such electronic surveillance shall be limited
in extent and duration to that necessary to determine
the existence and capability of such equipment, and that
any information acquired by such surveillance shall be
used only to enforce this chapter or section 605 of the
Communications Act of 1934 or to protect information
from unlawful electronic surveillance.

"(f) Nothing contained in this chapter, or section 605
of the Communications Act of 1934 (47 U.S.C. 605) shall
be deemed to affect the acquisition by the United States
Government of foreign intelligence information from inter-
national or foreign communications by a means other than
electronic surveillance as defined in section 2521 (b) (6)
of this title; and the procedures in this chapter and chapter
120 of this title, shall be the exclusive means by which
electronic surveillance, as defined in section 2521 (b) (6)
of chapter 120, and the interception of domestic wire and
oral communications may be conducted."

(d) Section 2511 (3) is repealed.

(e) Section 2515 is amended by inserting the words
"or electronic surveillance, as defined in chapter 120, has
been conducted" after the word "intercepted", by inserting
the words "or other information obtained from electronic
surveillance, as defined in chapter 120," after the second
appearance of the word "communication", and by inserting
"or chapter 120" after the final appearance of the word
"chapter".
(f) Section 2518 (1) is amended by inserting the words "under this chapter" after the word "communication".

(g) Section 2518 (4) is amended by inserting the words "under this chapter" after both appearances of the words "wire or oral communication".

(h) Section 2518 (9) is amended by striking the word "intercepted" and inserting the words "intercepted pursuant to this chapter" after the word "communication".

(i) Section 2518 (10) is amended by striking the word "intercepted" and inserting the words "intercepted pursuant to this chapter" after the first appearance of the word "communication".

(j) Section 2519 (3) is amended by inserting the words "pursuant to this chapter" after the words "wire or oral communications" and after the words "granted or denied".

(k) Section 2520 is amended by deleting all below subsection (2) and inserting in lieu thereof: "Any person other than a foreign power or an agent of a foreign power as defined in sections 2521 (b) (1) and 2521 (b) (2) (A) of chapter 120, who has been subject to electronic surveil-

lance, as defined in chapter 120, or whose wire or oral com-
munication has been intercepted, or about whom information
has been disclosed or used, in violation of this chapter, shall
(1) have a civil cause of action against any person who so
acted in violation of this chapter and”.

Passed the Senate April 20 (legislative day, February 6), 1978.

Attest: J. S. KIMMITT,
Secretary.