Whereas the Communist-controlled governments of the Soviet Union, Romania, and other Warsaw Pact nations have systematically sought to annihilate organized religions, especially the Byzantine Rite Catholic Church, by every possible means, including the imprisonment and or death of the Church hierarchy—the only Church leaders with authority to make decisions for the faithful;

Whereas no ecclesiastical document with canonical value exists calling for the dissolution of the Byzantine Rite Church, and no bishops have endorsed or agreed to any merger with the Orthodox Church, choosing instead intense suffering, persecution, and death at the hands of their captors;

Whereas even after brutal torture, intimidation, imprisonment, and threats against their families less than 40 of the considerbly more than 2,000 priests in Romania submitted to the pressure of the Government of Romania and even so continue to practice their faith;

Whereas 142 Byzantine Rite Catholic monasteries and convents, 4,119 churches and chapels in Ukraine, and countless other such facilities and Church properties were seized throughout Eastern Europe, including the Romanian Catholic cathedral at Blaj;

Whereas the Byzantine Rite and Latin Rite Catholic faithful in Ukraine, Romania, Czechoslovakia, and throughout Eastern Europe continue to profess and practice their faith despite a history of persecution which includes torture, imprisonment, harassment, and threats;

Whereas Byzantine Rite Catholic bishops and priests continue to be ordained and to serve the spiritual needs of the faithful in catacomb-like secrecy;

Whereas although the Soviet Union and its satellites wish the world to think that there are no Byzantine Rite Catholics within their borders, millions remain faithful to the Holy See and are conscientious, practicing Catholics and have asked their brethren in the West to plead for their religious freedom and the restoration of their Churches; and

Whereas the Government of the Soviet Union and the governments of other Soviet-bloc Eastern European countries refuse to allow the restoration of the Byzantine Rite Catholic Church on an equal basis with other recognized religions and refuse to restore all confiscated property of the Byzantine Rite Catholic Churches: Now, therefore, be it

Resolved, That (a) the Senate hereby recognizes the continuing right of the people of Ukraine, Lithuania, Romania, Czechoslovakia, and all other Soviet-bloc Eastern European countries to have freedom of religion.

(b) The Senate hereby deplores the refusal of the Soviet Union and Romania to officially recognize the Byzantine Rite Catholic Church and the refusal of the Soviet Union, Romania, and Czechoslovakia (which allowed the restoration of the Byzantine Rite Church in 1968) to restore all Church properties and possessions.

(c) It is the sense of the Senate that the President should instruct the United States delegation of the Review Meeting of the Conference on Security and Cooperation in Europe, scheduled for November 4, 1986, to press for the full restoration of the Byzantine Rite Catholic Church and freedom of religion for the people of all the Captive Nations before the world community.

SEC. 2. The Secretary of the Senate shall transmit a copy of this resolution to the President.

Mr. DOLE. Mr. President, I move to reconsider the vote by which the resolution was agreed to.

Mr. BYRD. I move to lay that motion on the table.

The motion to lay on the table was agreed to.

RELEASE TO MUSEUMS OF CERTAIN OBJECTS OF THE UNITED STATES INFORMATION AGENCY

The bill (H.R. 5522) to authorize the release to museums in the United States of certain objects owned by the United States Information Agency, was considered, ordered to a third reading, read the third time, and passed.

Mr. DOLE. Mr. President, I move to reconsider the vote by which the bill was passed.

Mr. BYRD. I move to lay that motion on the table.

The motion to lay on the table was agreed to.

CONCERNING THE SOVIET PERSECUTION OF MEMBERS OF THE UKRAINIAN AND OTHER PUBLIC HELSINKI MONITORING GROUPS

The concurrent resolution (S. Con. Res. 154) concerning the Soviet Union's persecution of members of the Ukrainian and other public Helsinki Monitoring Groups, was indefinitely postponed.

CONCERNING SOVIET PERSECUTION OF MEMBERS OF THE UKRAINIAN AND OTHER HELSINKI MONITORING GROUPS

The concurrent resolution (H. Con. Res. 332) concerning the Soviet Union's persecution of members of the Ukrainian and other public Helsinki Monitoring Groups, was considered, and agreed to.

The preamble was agreed to.

Mr. DOLE. Mr. President, I move to consider the vote by which the concurrent resolution was agreed to.

Mr. BYRD. I move to lay that motion on the table.

The motion to lay on the table was agreed to.

□ 1850

ELECTRONIC COMMUNICATIONS PRIVACY ACT

Mr. DOLE. Mr. President, I ask unanimous consent that the Senate now turn to Calendar No. 700, H.R. 4952, dealing with electronic communcations.

The PRESIDING OFFICER. The clerk will report.

The assistant legislative clerk read as follows:

A bill (H.R. 4952) to amend title 18, United States Code, with respect to the interception of certain communications other forms of surveillance, and for other purposes.

The PRESIDING OFFICER. Without objection, the Senate will proceed to its immediate consideration.

The Senate proceeded to consider the bill.

AMENDMENT NO. 3107

(Purpose: To insert a substitute amendment)

Mr. BYRD. Mr. President, on behalf of Senators LEAHY, MATHIAS, and THURMOND, I send an amendment to the desk and ask for its immediate consideration.

The PRESIDING OFFICER. The clerk will report.

The assistant legislative clerk read as follows:

The Senator from West Virginia [Mr. BYRD], for Mr. LEAHY (for himself and Mr. MATHIAS, and Mr. THURMOND), proposes an amendment numbered 3107, in the nature of a substitute.

Mr. BYRD. Mr. President, I ask unanimous consent that further reading of the amendment be dispensed with.

The PRESIDING OFFICER. Without objection, it is so ordered.

The amendment is as follows:

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

SECTION 1. SHORT TITLE.

This Act may be cited as the "Electronic Communications Privacy Act of 1986".

TITLE I—INTERCEPTION OF COMMUNICATIONS AND RELATED MATTERS

SEC. 101. FEDERAL PENALTIES FOR THE INTERCEPTION OF COMMUNICATIONS.

(a) DEFINITIONS.—(1) Section 2510(1) of title 18, United States Code, is amended—

(A) by striking out "any communication" and inserting "any aural transfer" in lieu thereof;

(B) by inserting "(including the use of such connection in a switching station)" after "reception".

(C) by striking out "as a common carrier" and

(D) by inserting before the semicolon at the end the following: "or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit".

(2) Section 2510(2) of title 18, United States Code, is amended by inserting before the semicolon at the end the following: ", but such term does not include any electronic communication".

(3) Section 2510(4) of title 18, United States Code, is amended—

(A) by inserting "or other" after "aural"; and

(B) by inserting ", electronic," after "wire".

(4) Section 2510(5) of title 18, United States Code, is amended in clause (a)(i) by inserting before the semicolon the following: "or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business".

(5) Section 2510(8) of title 18, United States Code, is amended by striking out "identity of the parties to such communication or the existence,".

(6) Section 2510 of title 18, United States Code, is amended—

(A) by striking out "and" at the end of paragraph (10);

(B) by striking out the period at the end of paragraph (11) and inserting a semicolon in lieu thereof; and

(C) by adding at the end the following:

"(12) 'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

"(A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

"(B) any wire or oral communication;

"(C) any communication made through a tone-only paging device; or

"(D) any communication from a tracking device (as defined in section 3117 of this title);

"(13) 'user' means any person or entity who—

"(A) uses an electronic communication service; and

"(B) is duly authorized by the provider of such service to engage in such use;

"(14) 'electronic communications system' means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

"(15) 'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications;

"(16) 'readily accessible to the general public' means, with respect to a radio communication, that such communication is not—

"(A) scrambled or encrypted;

"(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

"(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

"(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

"(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

"(17) 'electronic storage' means—

"(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

"(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and

"(18) 'aural transfer' means a transfer containing the human voice at any point between and including the point of origin and the point of reception.".

(b) EXCEPTIONS WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—

(1) Section 2511(2)(a)(ii) of title 18, United States Code, is amended—

(A) by striking out "violation of this subparagraph by a communication common carrier or an officer, employee, or agent thereof" and inserting in lieu thereof "such disclosure";

(B) by striking out "the carrier" and inserting in lieu thereof "such person"; and

(C) by striking out "an order or certification under this subparagraph" and inserting in lieu thereof "a court order or certification under this chapter".

(2) Section 2511(2)(d) of title 18, United States Code, is amended by striking out "or for the purpose of committing any other injurious act".

(3) Section 2511(2)(f) of title 18, United States Code, is amended—

(A) by inserting "or chapter 121" after "this chapter"; and

(B) by striking out "by" the second place it appears and inserting in lieu thereof ", or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing".

(4) Section 2511(2) of title 18, United States Code, is amended by adding at the end the following:

"(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

"(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

"(ii) to intercept any radio communication which is transmitted—

"(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

"(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

"(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

"(IV) by any marine or aeronautical communications system;

"(iii) to engage in any conduct which—

"(I) is prohibited by section 633 of the Communications Act of 1934; or

"(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

"(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

"(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

"(h) It shall not be unlawful under this chapter—

"(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

"(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.".

(c) TECHNICAL AND CONFORMING AMENDMENTS.—(1) Chapter 119 of title 18, United States Code, is amended—

(A) in each of sections 2510(5), 2510(8), 2510(9)(b), 2510(11), and 2511 through 2519 (except sections 2515, 2516(1) and 2518(10)), by striking out "wire or oral" each place it appears (including in any section heading) and inserting "wire, oral, or electronic" in lieu thereof; and

(B) in section 2511(2)(b), by inserting "or electronic" after "wire".

(2) The heading of chapter 119 of title 18, United States Code, is amended by inserting "and electronic communications" after "wire".

(3) The item relating to chapter 119 in the table of chapters at the beginning of part I of title 18 of the United States Code is amended by inserting "and electronic communications" after "Wire".

(4) Section 2510(5)(a) of title 18, United States Code, is amended by striking out "communications common carrier" and inserting "provider of wire or electronic communication service" in lieu thereof.

(5) Section 2511(2)(a)(i) of title 18, United States Code, is amended—

(A) by striking out "any communication common carrier" and inserting "a provider of wire or electronic communication service" in lieu thereof;

(B) by striking out "of the carrier of such communication" and inserting "of the provider of that service" in lieu thereof; and

(C) by striking out ": *Provided,* That said communication common carriers" and inserting ", except that a provider of wire communication service to the public" in lieu thereof.

(6) Section 2511(2)(a)(ii) of title 18, United States Code, is amended—

(A) by striking out "communication common carriers" and inserting "providers of wire or electronic communication service" in lieu thereof;

(B) by striking out "communication common carrier" each place it appears and inserting "provider of wire or electronic communication service" in lieu thereof; and

(C) by striking out "if the common carrier" and inserting "if such provider" in lieu thereof.

(7) Section 2512(2)(a) of title 18, United States Code, is amended—

(A) by striking out "a communications common carrier" the first place it appears and inserting "a provider of wire or electronic communication service" in lieu thereof; and

(B) by striking out "a communications common carrier" the second place it appears and inserting "such a provider" in lieu thereof; and

(C) by striking out "communications common carrier's business" and inserting "business of providing that wire or electronic communication service" in lieu thereof.

(8) Section 2518(4) of title 18, United States Code, is amended—

(A) by striking out "communication common carrier" in both places it appears and inserting "provider of wire or electronic communication service" in lieu thereof; and

(B) by striking out "carrier" and inserting in lieu thereof "service provider".

(d) PENALTIES MODIFICATION.—(1) Section 2511(1) of title 18, United States Code, is amended by striking out "shall be" and all that follows through "or both" and inserting in lieu thereof "shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5)".

(2) Section 2511 of title 18, United States Code, is amended by adding after the material added by section 102 the following:

"(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

"(b) If the offense is a first offense under paragraph (a) of this subsection and is not

for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled or encrypted, then—

"(i) if the communication is not the radio portion of a cellular telephone communication, a public land mobile radio service communication or a paging service communication, and the conduct is not that described in subsection (5), the offender shall be fined under this title or imprisoned not more than one year, or both; and

"(ii) if the communication is the radio portion of a cellular telephone communication, a public land mobile radio service communication or a paging service communication, the offender shall be fined not more than $500.

"(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted—

"(i) to a broadcasting station for purposes of retransmission to the general public; or

"(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

"(5)(a)(i) If the communication is—

"(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

"(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

"(ii) In an action under this subsection—

"(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

"(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

"(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.".

(e) EXCLUSIVITY OF REMEDIES WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—Section 2518(10) of title 18, United States Code, is amended by adding at the end the following:

"(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.".

(f) STATE OF MIND.—Paragraphs (a), (b), (c), and (d) of subsection (1) of section 2511 of title 18, United States Code, are amended by striking out "willfully" and inserting in lieu thereof "intentionally".

(2) Subsection (1) of section 2512 of title 18, United States Code, is amended in the matter before paragraph (a) by striking out "willfully" and inserting in lieu thereof "intentionally".

SEC. 102. REQUIREMENTS FOR CERTAIN DISCLOSURES.

Section 2511 of title 18, United States Code, is amended by adding at the end the following:

"(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

"(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

"(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

"(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

"(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

"(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.".

SEC. 103. RECOVERY OF CIVIL DAMAGES.

Section 2520 of title 18, United States Code, is amended to read as follows:

"§ 2520. Recovery of civil damages authorized

"(a) IN GENERAL.—Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

"(b) RELIEF.—In an action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages under subsection (c) and punitive damages in appropriate cases; and

"(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) COMPUTATION OF DAMAGES.—(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

"(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5)(a)(i) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and not more than $500.

"(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5)(a)(i) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1000.

"(2) In any other action under this section, the court may assess as damages whichever is the greater of—

"(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

"(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

"(d) DEFENSE.—A good faith reliance on—

"(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

"(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

"(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other law.

"(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.".

SEC. 104. CERTAIN APPROVALS BY JUSTICE DEPARTMENT OFFICIALS.

Section 2516(1) of title 18 of the United States Code is amended by striking out "or any Assistant Attorney General" and inserting in lieu thereof "any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division".

SEC. 105. ADDITION OF OFFENSES TO CRIMES FOR WHICH INTERCEPTION IS AUTHORIZED.

(a) WIRE AND ORAL INTERCEPTIONS.—Section 2516(1) of title 18 of the United States Code is amended—

(1) in paragraph (c)—

(A) by inserting "section 751 (relating to escape)," after "wagering information),";

(B) by striking out "2314" and inserting "2312, 2313, 2314," in lieu thereof;

(C) by inserting "the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities)," after "stolen property),";

(D) by inserting "section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire), section 1952B (relating to violent crimes in aid of racketeering activity)," after "1952 (interstate and foreign travel or transportation in aid of racketeering enterprises),";

(E) by inserting ", section 115 (relating to threatening or retaliating against a Federal official), the section in chapter 65 relating to destruction of an energy facility, and section 1341 (relating to mail fraud)," after "section 1963 (violations with respect to racketeer influenced and corrupt organizations)"; and

(F) by—

(i) striking out "or" before "section 351" and inserting in lieu thereof a comma; and

(ii) inserting before the semicolon at the end thereof the following: ", section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to

destruction of motor vehicles or motor vehicle facilities), or section 1992 (relating to wrecking trains)";

(2) by striking out "or" at the end of paragraph (g);

(3) by inserting after paragraph (g) the following:

"(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

"(i) any violation of section 1679a(c)(2) (relating to destruction of a natural gas pipeline) or subsection (i) or (n) of section 1472 (relating to aircraft piracy) of title 49, of the United States Code;

"(j) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act); or";

"(k) the location of any fugitive from justice from an offense described in this section;

(4) by redesignating paragraph (h) as paragraph (l); and

(5) in paragraph (a) by—

(A) inserting after "Atomic Energy Act of 1954)," the following: "section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel),";

(B) striking out "or" after "(relating to treason),"; and

(C) inserting before the semicolon at the end thereof the following: "chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy)".

(b) INTERCEPTION OF ELECTRONIC COMMUNICATIONS.—Section 2516 of title 18 of the United States Code is amended by adding at the end the following:

"(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.".

SEC. 106. APPLICATIONS, ORDERS, AND IMPLEMENTATION OF ORDERS.

(a) PLACE OF AUTHORIZED INTERCEPTION.—Section 2518(3) of title 18 of the United States Code is amended by inserting "(and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction)" after "within the territorial jurisdiction of the court in which the judge is sitting".

(b) REIMBURSEMENT FOR ASSISTANCE.—Section 2518(4) of title 18 of the United States Code is amended by striking out "at the prevailing rates" and inserting in lieu thereof "for reasonable expenses incurred in providing such facilities or assistance".

(c) COMMENCEMENT OF THIRTY-DAY PERIOD AND POSTPONEMENT OF MINIMIZATION.—Section 2518(5) of title 18 of the United States Code is amended—

(1) by inserting after the first sentence the following: "Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered."; and

(2) by adding at the end the following: "In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.".

(d) ALTERNATIVE TO DESIGNATING SPECIFIC FACILITIES FROM WHICH COMMUNICATIONS ARE TO BE INTERCEPTED.—(1) Section 2518(1)(b)(ii) of title 18 of the United States Code is amended by inserting "except as provided in subsection (11)," before "a particular description".

(2) Section 2518(3)(d) of title 18 of the United States Code is amended by inserting "except as provided in subsection (11)," before "there is".

(3) Section 2518 of title 18 of the United States Code is amended by adding at the end the following:

"(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

"(a) in the case of an application with respect to the interception of an oral communication—

"(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

"(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

"(iii) the judge finds that such specification is not practical; and

"(b) in the case of an application with respect to a wire or electronic communication—

"(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

"(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and

"(iii) the judge finds that such purpose has been adequately shown.

"(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.".

(4) Section 2519(1)(b) of title 18, United States Code, is amended by inserting "(including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title)" after "applied for".

SEC. 107. INTELLIGENCE ACTIVITIES.

(a) IN GENERAL.—Nothing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity.

(b) CERTAIN ACTIVITIES UNDER PROCEDURES APPROVED BY THE ATTORNEY GENERAL.—Nothing in chapter 119 or chapter 121 of title 18, United States Code, shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General of activities intended to—

(1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;

(2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978; or

(3) access an electronic communication system used exclusively by a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978.

SEC. 108. MOBILE TRACKING DEVICES.

(a) IN GENERAL.—Chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"§ 3117. Mobile tracking devices

"(a) IN GENERAL.—If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.

"(b) DEFINITION.—As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object.".

(b) CLERICAL AMENDMENT.—The table of contents at the beginning of chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"3117. Mobile tracking devices.".

SEC. 109. WARNING SUBJECT OF SURVEILLANCE.

Section 2232 of title 18, United States Code, is amended—

(1) by inserting "(a) PHYSICAL INTERFERENCE WITH SEARCH.—" before "Whoever" the first place it appears;

(2) by inserting "(b) NOTICE OF SEARCH.—" before "Whoever" the second place it appears; and

(3) by adding at the end the following:

"(c) NOTICE OF CERTAIN ELECTRONIC SURVEILLANCE.—Whoever, having knowledge that a Federal investigative or law enforcement officer has been authorized or has applied for authorization under chapter 119 to intercept a wire, oral, or electronic communication, in order to obstruct, impede, or prevent such interception, gives notice or attempts to give notice of the possible interception to any person shall be fined under this title or imprisoned not more than five years, or both.

"Whoever, having knowledge that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the Foreign Intelligence Surveillance Act (50 U.S.C. 1801, et seq.), in order to obstruct, impede, or prevent such activity, gives notice or attempts to give notice of the possible activity to any person shall be fined under this title or imprisoned not more than five years, or both.".

SEC. 110. INJUNCTIVE REMEDY.

(a) IN GENERAL.—Chapter 119 of title 18, United States Code, is amended by adding at the end the following:

"§ 2521. Injunction against illegal interception

"Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 119 of title 18, United States Code, is amended by adding at the end thereof the following:

"2521. Injunction against illegal interception.".

SEC. 111. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b) or (c), this title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

(b) SPECIAL RULE FOR STATE AUTHORIZATIONS OF INTERCEPTIONS.—Any interception pursuant to section 2516(2) of title 18 of the United States Code which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such interception occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

(1) the day before the date of the taking effect of State law conforming the applicable State statute with chapter 119 of title 18, United States Code, as so amended; or

(2) the date two years after the date of the enactment of this Act.

(c) EFFECTIVE DATE FOR CERTAIN APPROVALS BY JUSTICE DEPARTMENT OFFICIALS.—Section 104 of this Act shall take effect on the date of enactment of this Act.

TITLE II—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

SEC. 201. TITLE 18 AMENDMENT.

Title 18, United States Code, is amended by inserting after chapter 119 the following:

"CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

"Sec.
"2701. Unlawful access to stored communications.
"2702. Disclosure of contents.
"2703. Requirements for governmental access.
"2704. Backup preservation.
"2705. Delayed notice.
"2706. Cost reimbursement.
"2707. Civil action.
"2708. Exclusivity of remedies.
"2709. Counterintelligence access to telephone toll and transactional records.
"2710. Definitions.

"§ 2701. Unlawful access to stored communications

"(a) OFFENSE.—Except as provided in subsection (c) of this section whoever—

"(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

"(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

"(b) PUNISHMENT.—The punishment for an offense under subsection (a) of this section is—

"(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain—

"(A) a fine of not more than $250,000 or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

"(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

"(2) a fine of not more than $5,000 or imprisonment for not more than six months, or both, in any other case.

"(c) EXCEPTIONS.—Subsection (a) of this section does not apply with respect to conduct authorized—

"(1) by the person or entity providing a wire or electronic communications service;

"(2) by a user of that service with respect to a communication of or intended for that user; or

"(3) in section 2703, 2704 or 2518 of this title.

"§ 2702. Disclosure of contents

"(a) PROHIBITIONS.—Except as provided in subsection (b)—

"(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

"(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

"(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

"(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

"(b) EXCEPTIONS.—A person or entity may divulge the contents of a communication—

"(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

"(2) as otherwise authorized in section 2516, 2511(2)(a), or 2703 of this title;

"(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

"(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

"(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or

"(6) to a law enforcement agency, if such contents—

"(A) were inadvertently obtained by the service provider; and

"(B) appear to pertain to the commission of a crime.

"§ 2703. Requirements for governmental access

"(a) CONTENTS OF ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

"(b) CONTENTS OF ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

"(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

"(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

"(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena; or

"(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

"(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service—

"(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

"(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

"(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—(1)(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to any person other than a governmental entity.

"(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental entity—

"(i) uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury subpoena;

"(ii) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant;

"(iii) obtains a court order for such disclosure under subsection (d) of this section; or

"(iv) has the consent of the subscriber or customer to such disclosure.

"(2) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

"(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) of this section shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

"(e) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, or certification under this chapter.

"§ 2704. Backup preservation

"(a) BACKUP PRESERVATION.—(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

"(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

"(3) The service provider shall not destroy such backup copy until the later of—

"(A) the delivery of the information; or

"(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

"(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider—

"(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

"(B) has not initiated proceedings to challenge the request of the governmental entity.

"(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

"(b) CUSTOMER CHALLENGES.—(1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement—

"(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

"(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

"(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term 'delivery' has the meaning given that term in the Federal Rules of Civil Procedure.

"(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

"(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

"(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

"§ 2705. Delayed notice

"(a) DELAY OF NOTIFICATION.—(1) A governmental entity acting under section 2703(b) of this title may—

"(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

"(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

"(2) An adverse result for the purposes of paragraph (1) of this subsection is—

"(A) endangering the life or physical safety of an individual;

"(B) flight from prosecution;

"(C) destruction of or tampering with evidence;

"(D) intimidation of potential witnesses; or

"(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

"(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

"(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

"(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that—

"(A) states with reasonable specificity the nature of the law enforcement inquiry; and

"(B) informs such customer or subscriber—

"(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

"(ii) that notification of such customer or subscriber was delayed;

"(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

"(iv) which provision of this chapter allowed such delay.

"(6) As used in this subsection, the term 'supervisory official' means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

"(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a

provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

"(1) endangering the life or physical safety of an individual;

"(2) flight from prosecution;

"(3 destruction of or tampering with evidence;

"(4) intimidation of potential witnesses; or

"(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

"§ 2706. Cost reimbursement

"(a) PAYMENT.—Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

"(b) AMOUNT.—The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

"(c) The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

"§ 2707. Civil action

"(a) CAUSE OF ACTION.—Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate.

"(b) RELIEF.—In a civil action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages under subsection (c); and

"(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) DAMAGES.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000.

"(d) DEFENSE.—A good faith reliance on—

"(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

"(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

"(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

"(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

"§ 2708. Exclusivity of remedies

"The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

"§ 2709. Counterintelligence access to telephone toll and transactional records

"(a) DUTY TO PROVIDE.—A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

"(b) REQUIRED CERTIFICATION.—The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may request any such information and records if the Director (or the Director's designee) certifies in writing to the wire or electronic communication service provider to which the request is made that—

"(1) the information sought is relevant to an authorized foreign counterintelligence investigation; and

"(2) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

"(c) PROHIBITION OF CERTAIN DISCLOSURE.—No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

"(d) DISSEMINATION BY BUREAU.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

"(e) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made under subsection (b) of this section.

"§ 2710. Definitions for chapter

"As used in this chapter—

"(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

"(2) the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.".

(b) CLERICAL AMENDMENT.—The table of chapters at the beginning of part I of title 18, United States Code, is amended by adding at the end the following:

"121. Stored Wire and Electronic Communications and Transactional Records Access 2701".

SEC. 202. EFFECTIVE DATE.

This title and the amendments made by this title shall take effect ninety days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

TITLE III—PEN REGISTERS AND TRAP AND TRACE DEVICES

SEC. 301. TITLE 18 AMENDMENT.

(a) IN GENERAL.—Title 18 of the United States Code is amended by inserting after chapter 205 the following new chapter:

"CHAPTER 206—PEN REGISTERS AND TRAP AND TRACE DEVICES

"Sec.

"3121. General prohibition on pen register and trap and trace device use; exception.

"3122. Application for an order for a pen register or a trap and trace device.

"3123. Issuance of an order for a pen register or a trap or trace device.

"3124. Assistance in installation and use of a pen register or a trap and trace device.

"3125. Reports concerning pen registers and trap and trace devices.

"3126. Definitions for chapter.

"§ 3121. General prohibition on pen register and trap and trace device use; exception

"(a) IN GENERAL.—Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

"(b) EXCEPTION.—The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service—

"(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

"(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service, or with the consent of the user of that service.

"(c) PENALTY.—Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

"§ 3122. Application for an order for a pen register or a trap and trace device

"(a) APPLICATION.—(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chap-

ter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

"(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

"(b) CONTENTS OF APPLICATION.—An application under subsection (a) of this section shall include—

"(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

"(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

"§ 3123. Issuance of an order for a pen register or a trap and trace device

"(a) IN GENERAL.—Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that the attorney for the Government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

"(b) CONTENTS OF ORDER.—An order issued under this section—

"(1) shall specify—

"(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached;

"(B) the identity, if known, of the person who is the subject of the criminal investigation;

"(C) the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and

"(D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and

"(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.

"(c) TIME PERIOD AND EXTENSIONS.—(1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.

"(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.

"(d) NONDISCLOSURE OF EXISTENCE OF PEN REGISTER OR A TRAP AND TRACE DEVICE.—An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that—

"(1) the order be sealed until otherwise ordered by the court; and

"(2) the person owning or leasing the line to which the pen register or a trap and trace device is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

"§ 3124. Assistance in installation and use of a pen register or a trap and trace device

"(a) PEN REGISTERS.—Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

"(b) TRAP AND TRACE DEVICE.—Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 3123(b)(2) of this title. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished to the officer of a law enforcement agency, designated in the court, at reasonable intervals during regular business hours for the duration of the order.

"(c) COMPENSATION.—A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

"(d) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order under this chapter.

"(e) DEFENSE.—A good faith reliance on a court order, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law.

"§ 3125. Reports concerning pen registers and trap and trace devices

"The Attorney General shall annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice.

"§ 3126. Definitions for chapter

"As used in this chapter—

"(1) the terms 'wire communication', 'electronic communication', and 'electronic communication service' have the meanings set forth for such terms in section 2510 of this title;

"(2) the term 'court of competent jurisdiction' means—

"(A) a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals; or

"(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;

"(3) the term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

"(4) the term 'trap and trace device' means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted;

"(5) the term 'attorney for the Government' has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

"(6) the term 'State' means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.".

(b) CLERICAL AMENDMENT.—The table of chapters for part II of title 18 of the United States Code is amended by inserting after the item relating to chapter 205 the following new item:

"206. Pen Registers and Trap and Trace Devices ..... 3121".

SEC. 302. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b), this title and the amendments made by this title shall take effect ninety days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

(b) SPECIAL RULE FOR STATE AUTHORIZATIONS OF INTERCEPTIONS.—Any pen register or trap and trace device order or installation which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such order or installation occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

(1) the day before the date of the taking effect of changes in State law required in order to make orders or installations under Federal law as amended by this title; or

(2) the date two years after the date of the enactment of this Act.

SEC. 303. INTERFERENCE WITH THE OPERATION OF A SATELLITE.

(a) OFFENSE.—Chapter 65 of title 18, United States Code, is amended by inserting at the end the following:

"§ 1367. Interference with the operation of a satellite

"(a) Whoever, without the authority of the satellite operator, intentionally or maliciously interferes with the authorized operation of a communications or weather satellite or obstructs or hinders any satellite transmission shall be fined in accordance with this title or imprisoned not more than ten years or both.

"(b) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency or of an intelligence agency of the United States."

(b) CONFORMING AMENDMENT.—The table of sections for chapter 65 of title 18, United States Code, is amended by adding at the end the following new item:

"1367. Interference with the operation of a satellite.".

Mr. LEAHY. Mr. President, not long ago, a message was transmitted by first class mail, by wire, or by some form of wireless communications link. Each had its advantages and vulnerabilities. Each was regulated by separate legislation that provided a legal framework of appropriate privacy protection of the user. It was a neat and tidy world, in which private users, common carriers, and Government knew their rights and limits.

Today, Americans have at their fingertips a broad array or telecommunications and computer technology, including electronic mail, voice mail, electronic bulletin boards, computer storage, cellular telephones, video teleconferencing, and computer-to-computer links. These technological advances are wonderful. They make the lives of individual citizens easier and they promote American business.

Unfortunately, most people who use these new forms of technology are not aware that the law regarding the privacy and security of such communications is in tatters.

The primary law in this area is the Federal wiretap statute, title III of the Omnibus Crime Control and Safe Streets Act of 1968. When title III was written 18 years ago, Congress could barely contemplate forms of telecomunications and computer technology we are starting to take for granted today. Congress could not envision the dramatic changes in the telephone industry which we have witnessed in the last few years. Today, a phone call can be carried by wire, microwave, or fiber optics. Even a local call may follow an interstate path. And an ordinary phone call can be transmitted in different forms—digitized voice, data or video. In addition, since the divestiture of AT&T and deregulation, many different companies, not just common carriers, offer a wide variety of telephone and other communications services.

In short, technology and the structure of the communications industry have outstripped existing law.

Senate bill 2575, the Electronic Communications Privacy Act of 1986 which I introduced with Senator MATHIAS and which Senators THURMOND, STAFFORD, ANDREWS and DECONCINI have cosponsored, is designed to update title III of the Omnibus Crime Control and Safe Streets Act to provide a reasonable level of Federal privacy protection to these new forms of communication.

The substitute amendment Senators MATHIAS, THURMOND, and I are offering today to the House version of the Electronic Communications Privacy Act, H.R. 4952, is the culmination of 2 years of hard work with Congressmen KASTENMEIER and MOORHEAD and their staffs on the House Judiciary Subcommittee on Courts, Civil Liberties, and the Administration of Justice. We have also worked with the Department of Justice, the American Civil Liberties Union, representatives of the computer and telecommunications industry, the Federal Communications Commission, representatives of the satellite dish industry, and satellite dish owners, radio hobbyists, and technology and privacy groups. I want to thank all those people who have worked with me, with Senator MATHIAS and our staffs to make the Electronic Communications Privacy Act a better bill.

Let me describe the Electronic Communications Privacy Act briefly. It provides standards by which law enforcement agencies may obtain access to both electronic communications and the records of an electronic communications system. These provisions are designed to protect legitimate law enforcement needs while minimizing intrusions on the privacy of system users as well as the business needs of electronic communications system providers.

At the request of the Justice Department, we strengthened the current wiretap law from a law enforcement perspective. Specifically, we expanded the list of felonies for which a voice wiretap order may be issued and the list of Justice Department officials who may apply for a court order to place a wiretap. We also added a provision making it easier for law enforcement officials to deal with a target who repeatedly changes telephones to thwart interception of his communications, and created criminal penalties for those who notify a target of a wiretap in order to obstruct it.

The legislation creates a statutory framework for the authorization and issuance of orders for pen registers and trap and trace devices. It also creates civil penalties for the users of electronic communications services whose rights under the bill are violated. Finally, it preserves the careful balance governing electronic surveillance for foreign intelligence and counterintelligence purposes embodied in the Foreign Intelligence Surveillance Act of 1978. And it provides a clear procedure for access to telephone toll records in counterintelligence investigations.

Since we introduced S. 2575 in June, Senator MATHIAS and I have continued to improve this legislation, and the substitute we are offering today to H.R. 4952, the House-passed version of the Electronic Communications Act includes several important changes.

In order to address the recent Captain Midnight incident, at the request of the FCC, we added a provision to increase the penalties for the intentional or malicious interference with a satellite transmission.

We wanted to underscore that the inadvertent reception of a protected communication is not a crime. In order to do that, we changed the state of mind requirement under title III of the Omnibus Crime Control and Safe Streets Act from "willful" to "intentional."

Mr. President, as the Subcommittee on Patents, Copyrights and Trademarks prepared to markup S. 2575, Senators LAXALT, GRASSLEY, DECONCINI, GORE and SIMPSON expressed concerns about the bill's penalty structure for the interception of certain satellite transmissions by home viewers. In order to address those concerns we have completely restructured the penalty provisions of the bill for such conduct.

That restructuring is accomplished through Senator GRASSLEY's proposal which eliminates from the Electronic Communications Privacy Act, criminal penalties for the home viewing of private satellite video communications. Senators LAXALT, MCCONNELL, SIMPSON, and DENTON are cosponsors of the Grassley amendment.

The amendment is incorporated in the substitute we are offering today, and I would like to describe it briefly. The criminal penalties and civil liability provisions of chapter 119 of title 18 of the United States Code have been modified so that there is a two-track, tiered penalty structure for home viewing of private satellite transmissions when that conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain.

On the public side, a first offender would be subject to a suit by the Government for injunctive relief. If injunctive relief is granted, one who violates the injunction would be subject to the full panoply of enforcement mechanisms within the court's existing authority, including criminal and civil contempt. Second and subsequent offenses carry a mandatory $500 civil fine for each violation. The term "violation" in this context refers to each viewing of a private video communication.

On the private side, a person harmed by the private viewing of such a satellite communication may sue for damages in a civil action. If the defendant has not previously been enjoined in a Government action as described above, and has not previously been found liable in a civil suit, the plaintiff may recover the greater of his actual damages or statutory damages of $50 to $500. A second offender—one who has been found liable in a prior private civil action or one who has been enjoined in a government suit—is subject to liability for the greater of actual damages or statutory damages of $100 to $1,000. Third and subsequent offenders are subject to the bill's full civil penalties.

It also takes outside the penalty provisions of the Electronic Communications Privacy Act, the interception of a satellite transmission via audio subcarrier if the transmission is intended for redistribution to facilities open to the public, provided that the conduct is not for the purpose of direct or indirect commercial advantage or private financial gain. Audio subcarriers intended for redistribution to the public include those for redistribution by broadcast stations and cable and like facilities. They also include those for redistribution to buildings open to the public like hospitals and office buildings that pump in music which has been transmitted via subcarrier. As specified in the substitute, this audio subcarrier exclusion does not apply to data transmissions or to telephone calls.

The private viewing of satellite cable programming, network feeds and certain audio subcarriers will continue to be governed exclusively by section 705 of the Communications Act, as amended, and not by chapter 119 of title 18 of the United States Code.

Mr. President, this is a very good compromise. Those Senators who originally brought these concerns to our attention, are happy with it. So are the representatives of the satellite dish owners and manufacturers.

Senator SIMON expressed concerns that the Electronic Communications Privacy Act's penalties were too severe for the first offender who, without an unlawful or financial purpose, intercepts a cellular telephone call or certain radio communications related to news-gathering. Senator MATHIAS and I have accepted Senator SIMON's amendment, and it is incorporated in the substitute. The Simon amendment reduces the penalty for such an interception of an unencrypted, unscrambled cellular telephone call to a $500 criminal fine. Unencrypted, unscrambled radio communications transmitted on frequencies allocated under subpart D of part 74 of the FCC rules are treated like private satellite video communications are under Senator GRASSLEY's amendment.

Because we have been able to reach agreement on the Grassley and Simon amendments, there are no outstanding issues to be resolved.

I would like to thank all those who have worked with us to bring the Electronic Communications Privacy Act to the point of Senate passage. First, let me thank my principal cosponsor, Senator MATHIAS and his staff, Steve Metalitz and Ken Mannella. Senator THURMOND and his staff, Dennis Shedd and Cindy Blackburn have been very helpful.

I also would like to thank Congressman KASTENMEIER and MOORHEAD and the staff of the House Subcommittee on Courts, Civil Liberties and the Administration of Justice, David Beier, Deborah Leavy, and Joe Wolfe. Finally, I would like to thank my own staff, John Podesta, Ann Harkins and Tom Hodson.

Mr. President, let me just remind my colleagues in closing, that since the beginning of our national history, first class mail has preserved privacy while promoting commerce. Today a wide variety of new technology is used in American businesses and American homes side-by-side with first class mail. It is high time we updated our laws to bring them in line with that technology.

Mr. LEAHY. Mr. President, I ask unanimous consent that a summary of the Electronic Communications Privacy Act be printed in the RECORD at this point. This summary was prepared by the staff of the Senate Judiciary Committee's Subcommittee on Patents, Copyrights and Trademarks. Of course, the relevant legislative history is the Senate Judiciary Committee's report on S. 2575.

There being no objection, the summary was ordered to be printed in the RECORD, as follows:

A SUMMARY OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The Electronic Communications Privacy Act amends Title III of the Omnibus Crime Control and Safe Streets Act of 1968—the federal wiretap law—to protect against the unauthorized interception of electronic communications. The bill amends the 1968 law to update and clarify federal privacy protections and standards in light of dramatic changes in new computer and telecommunication technologies. Originally introduced in the Senate as S. 1667 by Senators Leahy and Mathias, and H.R. 3378 by Congressmen Kastenmeier and Moorhead, the bill has gone through a substantial revision as a result of negotiations with interested Senators and their staffs, various industry and privacy groups and the Department of Justice.

On June 11, the House Judiciary Committee unanimously reported H.R. 4952. On June 19, Senators Leahy and Mathias introduced that bill as S. 2575. On June 23, the House passed H.R. 4952. On August 12, the Subcommittee on Patents, Copyrights and Trademarks of the Senate Judiciary Committee reported S. 2575. During Subcommittee consideration some Senators expressed concern that the penalties for private viewing of certain satellite transmissions were too severe. Their concerns have been addressed by a reduction of the private and public penalties for home viewing. The bill also addresses the recent Captain Midnight incident by increasing penalties for interference with satellite transmissions.

The Justice Department strongly supports this bill. The Judiciary Committee reported S. 2575 on September 19.

Highlights of the Leahy-Mathias substitute to amend the Electronic Communications Privacy Act of 1986 follow.

Currently, Title III covers only voice communications. The bill expands coverage to include video and data communications.

Currently, Title III covers only common carrier communications. The bill eliminates that restriction since private carriers and common carriers perform so many of the same functions today that the distinction no longer serves to justify a different privacy standard.

At the request of the Justice Department, the bill continues to distinguish between electronic communications (data and video) and wire or oral communications (voice) for purposes of some of the procedural restrictions currently contained in Title III. For example, court authorization for the interception of a wire or oral communication may only be issued to investigate certain crimes specified in Title III. An interception of an electronic communication pursuant to court order may be utilized during the investigation of any federal felony.

Wire communications in storage, like voice mail, remain wire communications.

To underscore that the inadvertent reception of a protected communication is not a crime, the bill changes the state of mind requirement under Title III from "willful" to "intentional."

Certain electronic communications are exempted from the coverage of the bill including—

The radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

Tone-only paging devices;

Amateur radio operators and general mobile radio services;

Marine and aeronautical communications systems;

Police, fire, civil defense and other public safety radio communications systems;

Specific transmissions via audio subcarrier;

The satellite transmission of network feeds;

The satellite transmission of satellite cable programming as defined in Section 705 of the Communications Act of 1934;

Any other radio communication which is made through an electronic communications system that is configured so that such comunication is "readily accessible to the general public," a defined term in the bill.

The term readily accessible to the general public does not include communications made by cellular radio telephone systems; therefore, the bill continues current restrictions contained in Title III against the interception of telephone calls made on cellular telephone systems. However, the criminal penalty for an unlawful interception of cellular phone call and similar communications is reduced from the current five-year felony.

Under the Simon amendment that criminal penalty is reduced to a $500 fine.

The bill expands the list of felonies for which a voice wiretap order may be issued. It also expands the list of Justice Department officials who may apply for a court order to place a wiretap.

The bill creates a limited exception to the requirement that a wiretap order designate a specific telephone to be intercepted where the Justice Department makes a showing that the target of the wiretap is changing telephones to thwart interception of his or her communications.

A telephone company may move to quash an order for such a "roving tap" if compliance would be unduly burdensome.

The bill makes it a crime for a person who has knowledge of a court authorized wiretap to notify any person of the possible interception in order to obstruct, impede or prevent such interception.

Title II of the bill creates parallel privacy protection for the unauthorized access to the computers of an electronic communications system, if information is obtained or altered. It does little good to prohibit the unauthorized interception of information while it is being transmitted, if similar protection is not afforded to the information while it is being stored for later forwarding.

The bill establishes criminal penalties for any person who intentionally accesses without authorization a computer through

which an electronic communication service is provided and obtains, alters or prevents authorized access to a stored electronic communication. The offense is punished as a felony if committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain; otherwise it is punished as a petty offense.

Providers of electronic communication services to the public and providers of remote computing services to the public are prohibited from intentionally divulging the contents of communications contained in their systems except under circumstances specified in the bill.

The contents of messages contained in electronic storage of electronic communications systems which have been in storage for 180 days or less may be obtained by a government entity from the provider of the system only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent state warrant.

The content of messages stored more than 180 days and the contents of certain records stored by providers of remote computer processing services may be obtained from the provider of the service without notice to the subscriber if the government obtains a warrant under the Federal Rules of Criminal Procedure or with notice to the customer pursuant to an administrative subpoena, a grand jury subpoena, or a court order based on a showing that there is reason to believe that the contents of the communication are relevant to a legitimate law enforcement inquiry. Provisions for delay in notice are also included.

An electronic communications or remote computing service provider may disclose to a non-governmental entity customer information like mailing lists, but not the contents of the communication. Disclosure of such information to the government is required, but only when the government obtains a court order, warrant, subpoena, or customer consent.

At the FCC's request, a section was added to the bill to address problems highlighted by the recent Captain Midnight incident. The bill increases penalties for the intentional or malicious interference with satellite transmissions.

The bill clarifies that telephone companies and other service providers are not civilly or criminally liable for good faith assistance to law enforcement agencies.

Civil penalties are created for users of electronic communications services whose rights under the bill are violated.

The Grassley amendment, which the sponsors have accepted, sets up a reduced penalty structure for the private home viewer whose reception of specified satellite transmissions is not for commercial gain.

The Simon amendment, which the sponsors have accepted sets up the same penalty structure for the interception of radio communications transmitted on frequencies allocated under subpart D of part 74 of the FCC rules.

The penalty structure under the Grassley and Simon amendments is:

A first offender will be subject to a suit by the federal government for injunctive relief. If injunctive relief is granted, the court may use whatever means in its authority, including civil and criminal contempt, to enforce that injunction. It must impose a $500 civil fine. In addition, the penalty for second and subsequent offenses is a $500 fine in a suit brought by the government.

Under the private civil damages provisions of the bill, the first offender may be sued for the greater of actual damages or statutory damages of $50 to $500. The second offender is subject to suit for the greater of actual damages or statutory damages of $100 to $1000. Third and subsequent offenders are subject to full civil damages under the bill.

The bill creates a statutory framework for the authorization and issuance of an order for a pen register or a trap and trace device based on a finding that such installation and use is relevant to an on-going criminal investigation.

Mr. President, just very, very briefly, this Electronic Communications Privacy Act takes into consideration the fact that communications no longer are transmitted simply by wire. Now come communications are transmitted by computer, others in digitized form, and so forth.

This amendment is designed to bring the law concerning communications not only into the 20th century, but well into the 21st century.

Mr. President, I yield to the distinguished Senator from Maryland, the chairman of our subcommittee and a cosponsor with me on this amendment.

The PRESIDING OFFICER. The Senator from Maryland.

Mr. MATHIAS. Mr. President, today the Senate considers an important bill to enhance the privacy of Americans and update the provisions the 1968 wiretap act. The Electronic Communications Privacy Act of 1986, H.R. 4952, passed the House Judiciary Committee by a vote of 34 to 0. That bill was approved by the House by a voice vote on June 24.

The Subcommittee on Patents, Copyrights and Trademarks held hearings last fall on an earlier version of this legislation. In essence, the Electronic Communications Privacy Act responds to new developments in computer and communications technology by amending title III of the Omnibus Crime Control and Safe Streets Act of 1968—the Federal wiretap law—to protect against the unauthorized interception of electronic communications. Currently, title III covers only voice communications. The bill expands coverage of the wiretap act to include data and video communications on nearly the same basis as conventional telephone technology. In addition, the bill eliminates the distinction between common carrier communications and private carrier communications. S. 2575 extends privacy protection to new forms of electronic communications, but is careful to exempt media in which privacy is not expected, such as tone only paging devices; amateur radio services; police, fire, and other public safety radio communications systems; and many satellite transmissions, including network feeds destined for rebroadcast, and satellite cable programming as defined in section 705 of the Communications Act of 1934.

Since Senator LEAHY and I introduced the first version of this bill, S. 1667, the legislation has been substantially revised and improved. S. 2575, the companion bill to H.R. 4952, was reported by the Subcommittee on Patents Copyrights and Trademarks to the full Senate Judiciary Committee on August 12. Both the Senate and House versions of this important legislation enjoy the full support of the Justice Department, as well as major communications and computer industry groups and the American Civil Liberties Union.

Today, Senator LEAHY and I introduce an amendment to H.R. 4952 that incorporates the improvements in the bill made by the Subcommittee on Patents, Copyrights and Trademarks. This substitute amendment makes several minor and technical changes in the bill. Senator LEAHY has already placed a summary of this amendment in the RECORD. But I want to call the attention of my colleagues to the most important differences between the Senate and House versions of this important legislation.

First, the Federal Communications Commission has brought to our attention the problem they have encountered in a recent highly publicized case of "jamming" of satellite cable programming. The FCC has suggested a new provision to clarify and strengthen legal protection against deliberate or malicious interference with satellite transmissions. Senator THURMOND has suggested that this bill may be an appropriate vehicle for this important but noncontroversial change, and the subcommittee has agreed.

Second, a recurring concern throughout the consideration of this legislation has been the fear for inadvertent overhearing of electronic communications. The changes made by the House have gone a long way toward allaying this fear, but to drive the point home, this amendment provides that only intentional acts of interception—those meeting the highest standard of specific intent—can be published criminally.

Third, the Judiciary Committee has wrestled with another problem that was considered at length on the House side: Criminal liability for unencrypted radio signals, particular private satellite video transmissions.

The problem is to strike the right balance between privacy policy and the realities of physics. Individuals and businesses surely expect privacy when they participate in a private video-teleconference or, in the case of a television network, when they transmit raw news footage via satellite by a "backhaul feed." Certainly the law ought to enforce that expectation of privacy. At the same time, the engineers tell us that home satellite dishes may be able to receive some of this material, and that for truly private communications, encryption is a viable alternative.

This amendment contains substantial barriers to imposing liability on satellite dish owners: the exemption for cable programming and network feeds, for example, and the requirement of an intentional interception. But, at the urging of Senator LAXALT, Senator GRASSLEY, and others, we

have reexamined this issue. The amendment before the Senate provides a remedy for intentional interception of private video transmissions via satellite; but in a proceeding brought by the Government it would reduce that sanction to the lowest possible level—injunctive relief. It also provides for lower statutory damages in private suits involving interception of video transmissions via satellite than those imposed for other types of violations. We believe this strikes the right balance: It defines these interceptions as wrongful, but takes into account the equities on the other side of the issue. This is particularly true since these interceptions are already covered by section 705 of the Communications Act. The provisions in this legislation are in addition to any remedies that may be available to the Government or to a private party under the Communications Act.

Finally, the substitute amendment now before the Senate incorporates important changes suggested by Senator SIMON. One of those changes is the elimination of the 6-month jail term, included in the House-passed bill, for first offenders whose conduct is the interception of the cellular portion of a telephone call, when the offender has committed no act beyond listening to the contents of the call.

Many Senators have contributed to the development of this comprehensive privacy legislation. I have mentioned a few earlier in my remarks; however, I would like to take this opportunity to commend particularly the efforts of the Senator from Vermont [Mr. LEAHY] who has worked tirelessly on this proposal from its origination through its successful conclusion. In the other body, the chairman and ranking minority member of the House Judiciary Subcommittee on Courts, Civil Liberties, and the Administration of Justice, Representatives ROBERT KASTENMEIER and CARLOS MOORHEAD, have shown exemplary leadership on this issue, and I am confident that through their continued efforts, this important and innovative bill will soon arrive on the President's desk for signature.

Mr. THURMOND. Mr. President, today, I rise in support of the amendment to H.R. 4952, the Electronic Communications Privacy Act of 1986. The Leahy, Mathias, Thurmond substitute amendment is S. 2575, the Senate companion, which has been reported by the Judiciary Committee.

As a cosponsor of S. 2575, the Senate bill, I commend Senator PATRICK J. LEAHY and Senator CHARLES McC. MATHIAS, JR., for introducing this much-needed legislation. The bill is the product of over a year's worth of negotiations and is now strongly supported by business groups as well as the Justice Department.

This legislation updates present wiretap law which currently provides privacy protection only for voice communications that are transmitted in whole or part by wire by adding new protection for certain voice communications, regardless of how they are transmitted, as well as data communications and electronic mail.

This legislation is necessary due to the changes that have occurred in communications technology since the current law was enacted in 1968. Along with providing privacy protection for new forms of technology, this bill also clarifies the procedures that law enforcement officers must follow when they seek permission for a wiretap.

When S. 2575, was first introduced and referred to the committee, it contained a provision that would make it a criminal offense to intercept satellite communications—known as backhauls—which are transmissions between a television affiliate and the network, as well as video conferences transmitted by satellite. Concern has been expressed in the committee that such a provision may unfairly subject unknowing satellite dish owners to criminal liability. This amendment responds to this concern by providing that a person must intentionally intercept such communications to be subject to penalties, and those penalties will be civil only. This amendment also contains other changes which serve to strengthen this bill.

I believe that this amendment strikes a reasonable balance between legitimate privacy concerns and the importance of Federal officials using electronic surveillance as an effective and valuable law enforcement tool. Because this needed legislation is supported by all members of the Judiciary Committee, and because I have been informed that the essence of this Senate amendment will be maintained through conference, I am willing to support this expedited process. I urge each one of my colleagues to vote for this amendment, and support the amended bill.

Mr. President, the House has passed this legislation. The Senate Judiciary Committee considered it carefully. We approved it, and the report is here now in the Senate.

Mr. GRASSLEY. Mr. President, I am very pleased with the agreements we were able to reach concerning the provisions in this bill which relate to home dish users. First, we have affirmed the right of dish users to listen to all unencrypted audio subcarriers that are redistributed by facilities open to the public. This includes subcarriers meant for redistribution by broadcast stations, cable systems, and like facilities and those subcarriers made available in office buildings and other public places. Further, we have decriminalized the private noncommercial viewing of unscrambled satellite video programming that would have previously resulted in the imposition of criminal sanctions on people who simply view television in the privacy of their own homes.

Anyone who has actually viewed programming from a satellite Earth station will find that many channels are indistinguishable from one another in terms of network, nonnetwork, backhaul, or affiliate feeds. With dozens of sporting events, for example, it is difficult to tell whether one is watching a so-called affiliate feed or a backhaul feed. Similarly, with teleconferences, there is often little difference in screen format from own own hearing or Senate floor coverage.

Finally, by decriminalizing the private viewing of most satellite televisions signals, we avoid the problem of potentially invading the privacy of these people who watch television in their own homes.

The new sections regarding home dish viewing of private unencrypted satellite video transmissions provide for injunctive relief in the case of intentional viewing of such signals. Intentional viewing means that the Earth station owner must know that he is viewing a prohibited signal and that that type of viewing is not permited under the act.

So, in this case, the applicable remedy would be injunctive relief and, upon a second occurrence, a $500 civil penalty. This would give networks and other programmers the ability to claim protection under the act without scrambling their signals. These claims would largely be a fiction under any set of circumstances: however, I cannot see imposing criminal sanctions on an innocent viewing public for the benefit of those who could scramble but choose not to.

The new satellite dish provisions would affect 1.5 to 2 million American families nationwide who receive their television programming via satellite. Satellite dish technology is especially important to rural Americans who do not have the same access to a multiplicity of television programming as do their urban counterparts.

I wish to thank my colleagues, Senators LEAHY and MATHIAS, and their competent staffs for their diligent work on resolving the satellite dish issues.

Mr. DANFORTH. This legislation covers some conduct that also is prohibited under section 705 of the Communications Act of 1934. Do I understand correctly that the sanctions contained in this legislation would be imposed in addition to, and not instead of, those contained in section 705 of the Communications Act?

Mr. MATHIAS. That is correct. This legislation is not intended to substitute for any liabilities for conduct that also is covered by section 705 of the Communications Act. Similarly, it is not intended to authorize any conduct which otherwise would be prohibited by section 705. The penalties provided for in the Electronic Communications Privacy Act are in addition to those which are provided by section 705 of the Communications Act.

As a general rule, conduct which is illegal under section 705 of the Communications Act would also be illegal under this bill. These supplemental sanctions are particularly important where an unauthorized interception is made for direct or indirect financial gain. This bill is designed to help put an end to such conduct.

The exception to the general rule is that we do not provide liability for the noncommercial private viewing of unscrambled network feeds to affiliated stations by the owners of home satellite dishes. Accountability for that conduct will be determined solely under section 705 of the Communications Act. The private viewing of any other video transmissions not otherwise excepted by section 705(b) could be subject to action under both the Communications Act and this legislation.

Mr. DANFORTH. So although the proposed legislation which amends title 18 of the United States Code replaces, for specified conduct, the penalty structure of the Electronic Communications Privacy Act as introduced, and substitutes a scheme of public and private remedies under title 18, am I correct that conduct prohibited by the Communications Act will continue to be governed by that Act?

Mr. MATHIAS. That is correct. Conduct which is not prohibited by the Electronic Communications Privacy Act, but which is prohibited by the Communications Act, still will be subject to the full range of remedies and penalties under the Communications Act.

Mr. DANFORTH. I thank the distinguished Senator for this clarification.

Mr. DOLE. Mr. President, has the Leahy substitute been adopted?

The PRESIDING OFFICER. No, it has not. Is there further debate?

If not the question is on agreeing to the amendment.

The amendment (No. 3107) was agreed to.

Mr. DOLE. Mr. President, I move to reconsider the vote by which the amendment was agreed to.

Mr. BYRD. Mr. President, I move to lay that motion on the table.

The motion to lay on the table was agreed to.

The PRESIDING OFFICER. The bill is before the Senate and open to further amendment. If there be no further amendment to be proposed, the question is on the engrossment of the amendment and the third reading of the bill.

The amendment was ordered to be engrossed for a third reading and the bill to be read a third time.

The bill was read the third time.

The PRESIDING OFFICER. The bill having been read the third time, the question is, Shall it pass?

The bill (H.R. 4952), as amended, was passed.

Mr. DOLE. Mr. President, I move to reconsider the vote by which the bill, as amended, was passed.

Mr. MATHIAS. Mr. President, I move to lay that motion on the table.

The motion to lay on the table was agreed to.

REFERRAL OF S. 2575

Mr. DOLE. Mr. President, I ask unanimous consent that once the Judiciary Committee reports S. 2575, Electronic Communication Privacy Act, it be referred to the Commerce Committee for a period of 24 hours and at the end of that time, the committee be discharged, and the bill be placed on the calendar.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. DOLE. Mr. President, I further ask unanimous consent that if a conference on S. 2575, or the companion, H.R. 4952, is necessary, that two members of the Commerce Committee be included as Senate appointed conferees, for consideration of those matters that fall under the Commerce Committee jurisdiction.

The PRESIDING OFFICER. Without objection, it is so ordered.

COMPUTER FRAUD AND ABUSE ACT

Mr. DOLE. Mr. President, I ask unanimous consent that the Senate now turn to the consideration of Calendar 883, S. 2281, the Computer Fraud and Abuse Act.

The PRESIDING OFFICER. The clerk will report.

The assistant legislative clerk read as follows:

A bill (S. 2281) to amend title XVIII, United States Code, to provide additional penalties for fraud and related activities in connection with access devices and computers and further purposes.

The PRESIDING OFFICER. Is there objection to the immediate consideration of the bill?

There being no objection, the Senate proceeded to consider the bill which had been reported from the Committee on the Judiciary with amendments as follows:

(The parts of the bill intended to be stricken are shown in bold-faced brackets, and the parts of the bill intended to be inserted are shown in italics.)

S. 2281

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

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Fraud and Abuse Act of 1986".

SEC. 2. SECTION 1030 AMENDMENTS.

(a) MODIFICATION OF DEFINITION OF FINANCIAL INSTITUTION.—Section 1030(a)(2) of title 18, United States Code, is amended—

(1) by striking out "knowingly" and inserting "intentionally" in lieu thereof; and

(2) by striking out "as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.),".

(b) MODIFICATION OF EXISTING GOVERNMENT COMPUTERS OFFENSE.—Section 1030(a)(3) of title 18, United States Code, is amended *to read as follows*—

[(1) by striking out "knowingly" and inserting "intentionally" in lieu thereof;

[(2) by striking out ", or having accessed" and all that follows through "prevents authorized use of, such computer";

[(3) by striking out "It is not an offense" and all that follows through "use of the computer."; and

[(4) by striking out "if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation" and inserting in lieu thereof "if such computer is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, if such computer is used by or for the Government of the United States and such conduct affects such use".**]**

"(3) intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer;".

(c) MODIFICATION OF AUTHORIZED ACCESS ASPECT OF OFFENSES.—Paragraphs (1) and (2) of section 1030(a) of title 18, United States Code, are each amended by striking out ", or having accessed" and all that follows through "does not extend" and inserting "or exceeds authorized access" in lieu thereof.

(d) NEW OFFENSES.—Section 1030(a) of title 18, United States Code, is amended by inserting after paragraph (3) the following:

"(4) knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;

["(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters information in that computer, or prevents authorized use of that computer, and thereby causes loss to another of a value aggregating $1,000 or more during any one year period; or**]**

"(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby—

"(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

"(B) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

"(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

"(A) such trafficking affects interstate or foreign commerce; or

"(B) such computer is used by or for the Government of the United States;".

(e) ELIMINATION OF SECTION SPECIFIC CONSPIRACY OFFENSE.—Section 1030(b) of title 18, United States Code, is amended—

(1) by striking out "(1)"; and

(2) by striking out paragraph (2).

(f) PENALTY AMENDMENTS.—Section 1030 of title 18, United States Code, is amended—

(1) by striking out "of not more than the greater of $10,000" and all that follows through "obtained by the offense" in subsection (c)(1)(A) and inserting "under this title" in lieu thereof;

(2) by striking out "of not more than the greater of $100,000" and all that follows through "obtained by the offense" in subsection (c)(1)(B) and inserting "under this title" in lieu thereof;

(3) by striking out "or (a)(3)" each place it appears in subsection (c)(2) and inserting ", (a)(3) or (a)(6)" in lieu thereof;

(4) by striking out "of not more than the greater of $5,000" and all that follows through "created by the offense" in subsection (c)(2)(A) and inserting "under this title" in lieu thereof;

(5) by striking out "of not more than the greater of $10,000" and all that follows through "created by the offense" in subsection (c)(2)(B) and inserting "under this title" in lieu thereof;

(6) by striking out "not than" in subsection (c)(2)(B) and inserting "not more than" in lieu thereof;

(7) by striking out the period at the end of subsection (c)(2)(B) and inserting "; and" in lieu thereof; and

(8) by adding at the end of subsection (c) the following:

"(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

"(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph.".

(g) CONFORMING AMENDMENTS TO DEFINITIONS PROVISION.—Section 1030(e) of title 18, United States Code, is amended—

(1) by striking out the comma after "As used in this section" and inserting a one-em dash in lieu thereof;

(2) by aligning the remaining portion of the subsection so that it is cut in two ems and begins as an indented paragraph, and inserting "(1)" before "the term";

(3) by striking out the period at the end and inserting a semicolon in lieu thereof; and

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

"(2) the term 'Federal interest computer' means a computer—

"(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects [such use] *the use of the financial institution's operation or the Government's operation of such computer;* or

"(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;

"(3) the term 'State' includes the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States;

"(4) the term 'financial institution' means—

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal home loan bank system and any home loan bank; and

"(F) any institution of the Farm Credit System under the Farm Credit Act of 1971;

"(5) the term 'financial record' means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution; [and]

"(6) the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or [alter.".] *alter; and*

"(7) the term 'department of the United States' means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5.".

(h) LAW ENFORCEMENT AND INTELLIGENCE ACTIVITY EXCEPTION.—Section 1030 of title 18, United States Code, is amended by adding at the end the following new subsection:

"(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.".

Mr. DOLE. Mr. President, I move the committee amendments be agreed to en bloc.

The PRESIDING OFFICER. Is there objection to agreeing to the committee amendments en bloc? Without objection, it is so ordered.

The committee amendments were considered and agreed to en bloc.

AMENDMENT NO. 3108

Mr. DOLE. Mr. President, I send an amendment to the desk on behalf of Senators TRIBLE and LAXALT and ask for its immediate consideration.

The clerk will report.

The assistant legislative clerk read as follows:

The Senator from Kansas [Mr. DOLE], for Mr. TRIBLE and Mr. LAXALT, proposes an amendment numbered 3108.

Mr. DOLE. Mr. President, I ask unanimous consent that further reading of the amendment be dispensed with.

The PRESIDING OFFICER. Without objection, it is so ordered.

S. 2281 is amended—

1. In Section 2(b), by adding the term "(1)" before the words "to read as follows"; and

In Section 2(b), by adding at the end thereof the following new paragraph:

"(2) by striking out the flush language after section 1030(a)(3) of title 18, United States Code, beginning with "It is not an offense" and all that follows through "use of the computer.";

2. In Section 2(a), by adding at the end thereof the following new paragraph:

"(3) by striking out the term "or" where it appears at the end of section 1030(a)(2) of title 18."

3. In Section 2(f), by adding at the end thereof the following new paragraph:

"(9) by deleting the term "(b)(1)" where it appears in the first line of section 1030(c) of title 18 and inserting in lieu thereof the term "(b)"."

4. In Section 2(g), by adding to the list of terms to be defined as "financial institutions" the following:

"(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

"(H) the Securities Investor Protection Corporation."

5. In Section 2(a), by deleting the period at the end of paragraph (2) and inserting in lieu thereof a semicolon.

In Section 2(a), by adding at the end thereof the following new paragraph:

"(3) by adding after the term "financial institution" the following: "or of a card issuer as defined in section 1602(n) of Title 15,".

Mr. TRIBLE. Mr. President, I want to offer a small package of amendments to S. 2281, on behalf of myself and Senator LAXALT.

This amendment will make several minor changes in the bill. The first three changes are technical in nature and do not affect the substance of the legislation. The fourth change enlarges slightly the types of financial institutions whose computers will be protected by S. 2281, and I would like to explain this change briefly.

First, the amendment will extend the protections afforded by S. 2281 to computers belonging to broker-dealers who are registered with the securities and exchange commission. A similar change has already been made by the House of Representatives in passing its computer crime bill, and this simply makes an identical change.

Second, the amendment affords protection to the securities investor protection corporation. The SIPC is charged with insuring certain securities transactions. It does for securities what the FDIC and the FSLIC do for banking transactions. I am told by the Securities and Exchange Commission that the SIPC has a liability level of roughly $1 billion. Given the Federal Government's ultimate responsibility for that debt, I believe that the computers of the SIPC should be protected. I recognize that the SIPC is not traditionally recognized as a financial institution, and I want to make clear that it will be so defined only for purposes of including it within the ambit of S. 2281.

The fifth and last amendment will protect the computers of card issuers as defined in section 1602(n) of title 15. These entities are covered under the existing computer crime statute, 18 USC 1030(a)(2). They were inadvertently omitted from coverage because of a definitonal change made by S. 2281, and the Trible-Laxalt amendment simply restores their coverage under 18 USC 1030(a)(2).

The PRESIDING OFFICER. Is there further debate on the amendment? If not, the question is on agreeing to the amendment.

The amendment (No. 3108) was agreed to.

Mr. THURMOND. Mr. President, I am pleased that the Senate has turned its attention to S. 2281, the Computer

Fraud and Abuse Act sponsored by Senator TRIBLE.

This legislation is needed to address the real and growing danger of computer crime. Although Congress enacted a computer crime statute in 1984, that law was quite limited in scope. It provided criminal penalties only for stealing national security-related data, for trespassing onto Government computers, or for stealing computerized information on individuals' credit histories.

Because the 1984 statute was quite limited, there remains a great deal of computerized information that is wholly unprotected against computer crime. For the past 2 years, the Senate Judiciary Committee has tried to reach a consensus on how far to expand Federal jurisdiction over computer crime. The Subcommittee on Criminal Law held a hearing in October, 1985, on two computer crime measures: S. 440, sponsored by Senator TRIBLE, and S. 1678, which I sponsored at the request of the administration. In April of this year, the full Judiciary Committee held a hearing on S. 2281, a revised computer crime bill sponsored by Senator TRIBLE and Senator LAXALT. S. 2281 was reported unanimously by the Judiciary Committee on June 12, 1986.

This bill will clarify the 1984 statute to make clear that acts of simple trespass by unauthorized users of Government computers are punishable. It will also proscribe acts of fraud via computer or intentional destruction of computer data. Both fraud and destruction of property will be covered by S. 2281 when they are committed against computers belonging to the Federal Government or to federally insured financial institutions. The same offenses will be covered when the crime itself is interstate in nature. Finally, S. 2281 will permit prosecution of those who traffic in computer passwords belonging to others.

Mr. President, I believe the Senate must act quickly to give Federal prosecutors the tools they need to respond to computer-related crimes. S. 2281 will accomplish that goal, and I urge its adoption by the Senate.

Mr. DENTON. Mr. President, I rise today to express my strong support for S. 2281, the Computer Fraud and Abuse Act of 1986. I am pleased to be an original cosponsor of the bill, which was introduced by my distinguished colleague from Virginia, Senator TRIBLE, whom I congratulate and commend for his leadership on this issue.

Mr. President, the explosive growth and development of computer technology in recent years has left Government and many businesses vulnerable to new and highly sophisticated forms of criminal activities. Such crimes involve the use of computers to steal from, defraud, and vandalize government, agencies, banks and other businesses, schools, and other entities whose operations depend heavily upon the use of computers.

As an American Bar Association survey revealed last year, nearly one-half of American businesses and government agencies had been the victims of computer crime during the previous 12-month period. Such crimes resulted in known financial losses as high as $730 million, a figure which does not include crimes which go unreported either because they are not detected or because companies are reluctant to disclose the vulnerabilities of their computer systems.

Especially ominous is the threat which computer crime poses to financial institutions and sensitive Government operations. Today, electronic transfers of funds among banks is routine, and computer fraud, trespass, and theft could wreak havoc in this process. Furthermore, a computer criminal who gains access to classified Government information could thereby jeopardize the national security.

The rapid evolution of computer technology has required us on several occasions to reassess the adequacy of our existing criminal statutes to deal with the novel patterns of criminal activity made possible by the widespread use of computers. For instance, in June 1985, as chairman of the Senate Judiciary Subcommittee on Security and Terrorism, I chaired a hearing on the use of computers to transmit material that incites crime and constitutes interstate transmission of implicitly obscene matter. That hearing yielded abundant evidence of various courses of criminal conduct which were difficult or impossible to prosecute under existing law because the conduct occurs, in whole or in part, through computer transmissions.

The legislation before us today, S. 2281, is intended to ensure that our criminal justice system will be equal to the task of combating these new patterns of criminal activity. The bill is designed specifically to deal with crimes spawned by the computer age.

S. 2281 clarifies and strengthens existing Federal protections against computer crime. The bill makes it clear that unauthorized access to a Government computer is a trespass offense, as surely as if the offender had entered a restricted Government compound without proper authorization. The bill also broadens Federal privacy protections for data relating to individuals' credit histories to include the computerized records of all customers—individual and corporate—of federally insured financial institutions.

The bill creates new offenses to deal with certain acts which are not now crimes under Federal law, such as theft by computer with the intent to defraud and the intentional destruction of computer property, when those offenses are committed on an interstate basis or involve the computers of federally insured financial institutions.

S. 2281 addresses computer crimes which are properly matters of Federal concern. The legislation is needed to keep our Criminal Code relevant to such criminal activities, which are made possible by the continually developing technology in the computer field. I urge my colleagues to vote for passage of this timely and much-needed legislation.

Thank you, Mr. President.

Mr. LAXALT. Mr. President, I enthusiastically support S. 2281, the Computer Fraud and Abuse Act of 1986. This bill is the result of more than 2 years of careful deliberation and review by members of both the House and the Senate Committees on the Judiciary. In this Chamber, my good friend from Virginia, PAUL TRIBLE, took the lead in seeking the best possible means for addressing the problems posed in this country by computer crime. S. 2281 is largely his handiwork, and I am pleased to be a cosponsor of the bill.

The bill primarily does two things: First, it carefully extends Federal criminal jurisdiction to several types of conduct not presently covered by Federal law; and, second, the bill amends and adjusts several provisions of current law in order to respond to the suggestions of experts in the field and of the attorneys in the Department of Justice. S. 2281 does not represent the furthest possible reach of Federal jurisdiction in this area: it is not intended to. It is the general belief of the sponsors of this bill and of the Department of Justice that in this rapidly changing area of computer technology, the best legislative approach is to proceed cautiously, to address effectively known evils of computer misuse, and not to attempt to enact comprehensive or exhaustive computer crime legislation at this time. I fully expect Congress to continue to review the problems caused by computer fraud and abuse and to respond to them with appropriate remedies.

In this legislation, Senator TRIBLE and we on the Judiciary Committee attempted to respond to the suggestions and the advice of as many computer and legal experts as possible. We believed that computer crime legislation should be devised to deter the misuse of three sets of computers: computers owned or operated by or for the Federal Government, computers owned or operated by the Nation's financial institutions, and computer systems operating in two or more States where the law enforcement resources of State and local governments may be inadequate to address the multistate scope of the misconduct.

These three sets of computers are not treated identically. We attempted to deter misuse of Government computers as completely as possible. In the other two sets of computers, we attempted to address the most serious forms of abuse. Clearly, Congress will be open to further adjustment of the law covering these latter two sets just as Congress was willing to amend the

1984 statute in light of its practical effect.

I would like to make just one more point, Mr. President. We have tried to establish the most complete legislative history possible to provide information about the intended meaning of the legislative language before us today. The committee reports of the Senate and the House Committees on the Judiciary and the floor statements and section-by-section analyses that accompanied the introduction of S. 2281 on April 10, 1986, provide an excellent background for the new statutes. Because of the complexity of the subject matter, we wanted to be as certain as we could that the limits and the intended scope of this bill be clear to prosecutors and computer users alike. I believe that we accomplished that goal, and I thank my colleague from Virginia, Senator TRIBLE, and also the excellent chairman of the Committee on the Judiciary, Senator THURMOND, for their efforts in this regard.

In sum, I strongly support this legislation, and I urge my colleagues to do so here today. This legislation is timely and it is necessary. Senator TRIBLE and Representative BILL HUGHES should be commended for their excellent work.

Mr. TRIBLE. Mr. President, I am pleased that the Senate has turned its attention to S. 2281, a bill I have sponsored to enact new criminal penalties for computer-related crimes.

This legislation culminates several years of effort by the Congress to prevent the Nation's criminal laws from becoming obsolete, and to ensure that our criminal justice system is capable of addressing the types of offenses that have accompanied the rise of new technologies.

For some time, our criminal laws lagged behind technological innovation, specifically innovations in computer technology. Prosecutors at both the Federal and State levels have had difficulty adapting older criminal statutes—many of which were written before the advent of computer technology—to computer crimes. As a consequence, the vast array of computer data relied upon by government, businesses, and individuals has been largely unprotected against criminal misconduct.

During the past decade, many States have tackled this problem. Roughly 35 States now have some form of computer crime law on the books, including my own State of Virginia. The Federal Government, too, now penalizes some types of computer crime. Under legislation approved by the Congress in 1984, it is a Federal offense to steal national security-related data via computer, to trespass onto Government computers without authorization, or to steal data relating to individuals' credit histories.

These State and Federal actions are welcome. Yet, there remains an enormous amount of computerized data wholly unprotected against acts of theft, vandalism, and trespass. In the Government's race to protect this computer data against crime, the hour is late. Quite simply, the criminals have the technological edge.

Mr. President, it is time to dispel the notion that computer crime is a game, or a challenge to be overcome. The fact is, the computer criminal is a lawbreaker just like any other, and deserves to be treated as such.

To that end, I introduced legislation early in 1985 to strengthen Federal penalties for computer-related crime. That bill, S. 440, was the subject of hearings before the Senate Subcommittee on Criminal Law last October. Since then, I have worked closely with the Chairman of that subcommittee, Senator LAXALT, to reach a consensus on the proper scope of Federal jurisdiction over computer crime. The bill before us, S. 2281, embodies that consensus and was reported unanimously by the Senate Judiciary Committee in June.

This bill will assert Federal jurisdiction over computer crimes only in those cases in which there is a compelling Federal interest. This reflects my belief and the Judiciary Committee's belief that the States can and should handle most such crimes, and that Federal jurisdiction in this area should be asserted narrowly. To accomplish that, S. 2281 will increase the protections currently afforded computers belonging to the Federal Government, it will provide similar protections to computers belonging to federally insured financial institutions, and it will proscribe certain crimes that are interstate in nature.

Mr. President, for the past two decades, the United States has experienced a technological revolution. Widespread computer use has brought a great many benefits to American business and to all of our lives. But it has also created a new type of criminal—one who uses computers to steal, to defraud, and to abuse the property of others.

I believe it is time for the Congress to give Federal prosecutors the tools to respond to computer crime. S. 2281 will do so, and I urge my colleagues to join me in supporting this bill.

I also want to extend my special thanks to Senator LAXALT. He has been most helpful in fashioning this legislation and in guiding it through the Judiciary Committee, and I deeply appreciate his leadership. In addition, I want to thank the other cosponsors of S. 2281 for their valuable help—Senators DENTON, ARMSTRONG, STEVENS, ABDNOR, GLENN, and DIXON.

The PRESIDING OFFICER. The bill is before the Senate and open to further amendment. If there be no further amendment to be proposed, the question is on the engrossment and third reading of the bill.

The bill was ordered to be engrossed for a third reading, was read the third time, and passed, as follows:

S. 2281

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

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Fraud and Abuse Act of 1986".

SEC. 2. SECTION 1030 AMENDMENTS.

(a) MODIFICATION OF DEFINITION OF FINANCIAL INSTITUTION.—Section 1030(a)(2) of title 18, United States Code, is amended—

(1) by striking out "knowingly" and inserting "intentionally" in lieu thereof;

(2) by striking out "as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.),";

(3) by striking out the term "or" where it appears at the end of section 1030(a)(2) of title 18; and

(4) by adding after the term "financial institution" the following: "or of a card issuer as defined in section 1602(n) of Title 15,".

(b) MODIFICATION OF EXISTING GOVERNMENT COMPUTERS OFFENSE.—Section 1030(a)(3) of title 18, United States Code, is amended

(1) to read as follows—

"(3) intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer;".

(2) by striking out the flush language after section 1030(a)(3) of title 18, United States Code, beginning with "It is not an offense" and all that follows through "use of the computer.";

(c) MODIFICATION OF AUTHORIZED ACCESS ASPECT OF OFFENSES.—Paragraphs (1) and (2) of section 1030(a) of title 18, United States Code, are each amended by striking out ", or having accessed" and all that follows through "does not extend" and inserting "or exceeds authorized access" in lieu thereof.

(d) NEW OFFENSES.—Section 1030(a) of title 18, United States Code, is amended by inserting after paragraph (3) the following:

"(4) knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;

"(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby—

"(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

"(B) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

"(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

"(A) such trafficking affects interstate or foreign commerce; or

"(B) such computer is used by or for the Government of the United States;".

(e) ELIMINATION OF SECTION SPECIFIC CONSPIRACY OFFENSE.—Section 1030(b) of title 18, United States Code, is amended—

(1) by striking out "(1)"; and

(2) by striking out paragraph (2).

(f) PENALTY AMENDMENTS.—Section 1030 of title 18, United States Code, is amended—

(1) by striking out "of not more than the greater of $10,000" and all that follows through "obtained by the offense" in subsection (c)(1)(A) and inserting "under this title" in lieu thereof;

(2) by striking out "of not more than the greater of $100,000" and all that follows through "obtained by the offense" in subsection (c)(1)(B) and inserting "under this title" in lieu thereof;

(3) by striking out "or (a)(3)" each place it appears in subsection (c)(2) and inserting ", (a)(3) or (a)(6)" in lieu thereof;

(4) by striking out "of not more than the greater of $5,000" and all that follows through "created by the offense" in subsection (c)(2)(A) and inserting "under this title" in lieu thereof;

(5) by striking out "of not more than the greater of $10,000" and all that follows through "created by the offense" in subsection (c)(2)(B) and inserting "under this title" in lieu thereof;

(6) by striking out "not than" in subsection (c)(2)(B) and inserting "not more than" in lieu thereof;

(7) by striking out the period at the end of subsection (c)(2)(B) and inserting "; and" in lieu thereof; and

(8) by adding at the end of subsection (c) the following:

"(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

"(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph.".

(9) by deleting the term "(b)(1)" where it appears in the first line of section 1030(c) of title 18 and inserting in lieu thereof the term "(b)".

(g) CONFORMING AMENDMENTS TO DEFINITIONS PROVISION.—Section 1030(e) of title 18, United States Code, is amended—

(1) by striking out the comma after "As used in this section" and inserting a one-em dash in lieu thereof;

(2) by aligning the remaining portion of the subsection so that it is cut in two ems and begins as an indented paragraph, and inserting "(1)" before "the term";

(3) by striking out the period at the end and inserting a semicolon in lieu thereof; and

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

"(2) the term 'Federal interest computer' means a computer—

"(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or

"(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;

"(3) the term 'State' includes the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States;

"(4) the term 'financial institution' means—

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal home loan bank system and any home loan bank;

"(F) any institution of the Farm Credit System under the Farm Credit Act of 1971;

"(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934; and

(H) the Securities Investor Protection Corporation.

"(5) the term 'financial record' means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

"(6) the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter; and

"(7) the term 'department of the United States' means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5.".

(h) LAW ENFORCEMENT AND INTELLIGENCE ACTIVITY EXCEPTION.—Section 1030 of title 18, United States Code, is amended by adding at the end the following new subsection:

"(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.".

Mr. DOLE. Mr. President, I move to reconsider the vote by which the bill, as amended, was passed.

Mr. BYRD. Mr. President, I move to lay that motion on the table.

The motion to lay on the table was agreed to.

PROVIDING FOR THE REPLACEMENT OF CERTAIN LANDS WITHIN THE GILA BEND INDIAN RESERVATION

Mr. DOLE. Mr. President, I ask unanimous consent that the Senate now turn to consideration of H.R. 4216, dealing with settlement of the Papago Tribe, now being held at the desk.

The PRESIDING OFFICER. The clerk will report.

The assistant legislative clerk read as follows:

A bill (H.R. 4216) to provide for the replacement of certain lands within the Gila Bend Indian Reservation and for other purposes.

The PRESIDING OFFICER. Is there objection to the immediate consideration of the bill?

There being no objection, the Senate proceeded to consider the bill.

Mr. DECONCINI. Mr. President, I am a cosponsor of legislation introduced by my distinguished colleague, Mr. GOLDWATER, S. 2105, the Gila Bend Indian water settlement legislation. The companion legislation in the House, H.R. 4216, sponsored by Congressman UDALL and Congressman MCCAIN, passed the House on September 16, 1986. That legislation is being held at the desk in the Senate and like my colleague from Arizona, Mr. GOLDWATER, I ask that the House bill, H.R. 4216, be considered and passed by this body in lieu of S. 2105.

The Gila Bend Indian water settlement will settle all claims of the Tohono O'Odam Nation against the Federal Government for the harm caused to the Gila Bend Reservation as a result of the operation of Painted Rock Dam, a Corps of Engineers structure. Repeated flooding of the Gila Bend Reservation from the operation of the Painted Rock Dam has literally rendered the tribal lands within the reservation useless for agricultural purposes. Additionally, there has been a very high incidence of disease such as hypertension and kidney disorders because of the high salt content in the drinking water. Many believe this is attributable to flooding of lands in the entire Gila Bend area.

The Tohono O'Odam Nation has suffered both economically and psychologically because of the failure of the Federal Government to take action which could remedy this situation. As the trustee for Indian lands and people, the Secretary of the Interior has a responsibility to see that those residing in Indian country do not continue to suffer. This legislation will remedy the longstanding problems associated with the construction of the Painted Rock Dam.

The Gila Bend Reservation was established by President Chester Arthur in 1882 for the Papago Indians—currently known as the Tohono O'Odams—living in the Gila Bend area. Presently there are about 800 tribal members living in an area of approximately 10,297 acres. In 1949, the Secretary of the Interior approved an economic development plan for the Tohono O'Odam Nation which included the irrigation of 1,200 acres of farmland on the Gila Bend Reservation. About 3 months after the Papago Development Program was published, the Secretary of the Interior approved a request by the U.S. Army Corps of Engineers to construct a flood control dam on the Gila River 10 miles downstream of the Gila Bend Reservation. Before construction of the dam could take place, the corps had to obtain a flowage easement of 7,700 acres of reservation land from the Papago Tribe. However, prior to the tribe agreeing to the taking of its reservation land for a flowage easement, the corps went ahead with the construction of the Painted Rock Dam and completed the structure in 1960. At that time, the

corps and the BIA indicated that there would be infrequent flooding of the reservation lands that would not impair the tribe's ability to farm the land within the flowage easement.

Three years later, the U.S. Geological Survey, after conducting an investigation of water supply and irrigation potential in the Gila Bend area, concluded that full operation of the Painted Rock Dam would inundate the entire Gila Bend Reservation. Consequently, the first major flooding of the reservation occurred in 1978-79 and reoccurred in 1981, 1983 and 1984. Each time the extent and duration of the flooding was much greater than anticipated when the dam was authorized. Eventually, the reservation became unusable for economic purposes. Dense saltcedar from the flooding grew larger, and the reservation lost all productive capacity.

Recognizing the economic difficulties facing the Tohono O'Odam Tribe because of the flooding, the Congress, when it enacted the Southern Arizona Water Rights Settlement Act of 1982, authorized the Bureau of Indian Affairs to conduct a study of the reservation and directed the Secretary of the Interior to find suitable lands for a tribal reservation. The BIA completed its study in October 1983 and found that because of repeated flooding, silt deposition and saltcedar infestation, the Gila Bend Reservation has become unusable. The Secretary's search to find suitable Federal lands to replace the reservation lands from within a 100-mile radius of the reservation proved unsuccessful. After many discussions with the Department of the Interior and attempts at negotiations for a settlement, the tribe came to Congress with a proposed legislative settlement. That settlement, although subtantially modified from the earlier proposals, is now embodied in the provisions of H.R. 4216.

The Gila Bend settlement will allow the Tohono O'Odam Nation to locate and develop 9,880 acres of replacement land to be held in trust by the Secretary of the Interior. The Federal Government will provide the tribe with $30 million plus interest for the purpose of obtaining replacement lands, $10 million will be made available to the tribe each year over a 3-year period. The replacement lands will be found in Arizona by the tribe but must be outside the corporate limits of any city or town and outside the boundaries of the counties of Maricopa, Pinal and Pima. In exchange, the tribe will assign all rights to the 9,880 acres of land comprising the Gila Bend Reservation to the United States and waive all claims against the Federal Government for harm suffered by the tribe and its members. If private lands are acquired by the tribe, the Secretary of the Interior shall pay in-lieu taxes to the local governments.

While this may seem a large amount of money in these times of spiraling deficits, I am convinced that it will save the taxpayers millions of dollars in the long-run in litigation and lengthy court time. It will allow the Tohono O'Odam Nation to find suitable replacement lands and develop those lands for the economic well-being of its tribal members. It will also release the Government from any tribal claims to water from the Gila River. It is a fair and just settlement that has been hammered out by the tribe, Mr. UDALL and Mr. MCCAIN, and one which I feel is in the best interest of the tribe and the Federal Government.

I support H.R. 4216 in its present form and urge its adoption by the full Senate. Over 3 years of work have gone into this settlement and Congressman UDALL and Congressman MCCAIN have contributed substantially to bringing about this settlement. Additionally, Mr. Michael Jackson, professional staff of House Interior Committee, as well as other staffs, have spent a great deal of time on trying to develop a fair and reasonable settlement. I want to thank my colleagues and the staffs involved for forging a compromise which is acceptable to this Senator.

The PRESIDING OFFICER. The bill is before the Senate and open to amendment. If there be no amendment to be offered, the question is on the third reading and passage of the bill.

The bill (H.R. 4126) was ordered to a third reading, was read the third time and passed.

Mr. DOLE. Mr. President, I move to reconsider the vote by which the bill was passed.

Mr. BYRD. Mr. President, I move to lay that motion on the table.

The motion to lay on the table was agreed to.

PROVIDING FOR THE SETTLEMENT OF CERTAIN CLAIMS OF THE PAPAGO TRIBE OF ARIZONA ARISING FROM THE CONSTRUCTION OF THE TAT MOMOLIKOT DAM

Mr. DOLE. Mr. President, I ask unanimous consent that the Senate now turn to the consideration of H.R. 4217, dealing with certain claims of the Papago Tribe being held at the desk.

The PRESIDING OFFICER. The clerk will report the bill.

The assistant legislative clerk read as follows:

A bill (H.R. 4217) to provide for the settlement of certain claims of the Papago Tribe of Arizona arising from the construction of Tat Momolikot Dam, and for other purposes.

The PRESIDING OFFICER. Without objection, the Senate will proceed to its immediate consideration.

The Senate proceeded to consider the bill.

The PRESIDING OFFICER. The bill is before the Senate and is open to amendment. If there be no amendment to be offered, the question is on the third reading and passage of the bill.

The bill (H.R. 4217) was ordered to a third reading, was read the third time and passed.

Mr. DOLE. Mr. President, I move to reconsider the vote by which the bill was passed.

Mr. BYRD. Mr. President, I move to lay that motion on the table.

The motion to lay on the table was agreed to.

STEVENSON-WYDLER TECHNOLOGY INNOVATION ACT AMENDMENTS

Mr. DOLE. Mr. President, I ask that the Chair lay before the Senate a message from the House of Representatives on H.R. 3373.

The PRESIDING OFFICER laid before the Senate the following message from the House of Representatives:

Resolved, That the House disagree to the amendments of the Senate to the bill (H.R. 3773) entitled "An Act to amend the Stevenson-Wydler Technology Innovation Act of 1980 to promote technology transfer by authorizing Government-operated laboratories to enter into cooperative research agreements and by establishing a Federal Laboratory Consortium for Technology Transfer within the National Science Foundation, and for other purposes", and ask a conference with the Senate on the disagreeing votes of the two Houses thereon.

Ordered, That Mr. Fuqua, Mr. Walgren, Mr. Lundine, Mr. Lujan, and Mr. Boehlert be the managers of the conference on the part of the House.

Mr. DOLE. Mr. President, I move that the Senate insist on its amendments and agree to the conference requested by the House and that the Chair be authorized to appoint conferees on the part of the Senate.

The motion was agreed to, and the Presiding Officer appointed Mr. DANFORTH, Mr. GORTON, Mr. PRESSLER, Mr. HOLLINGS, and Mr. RIEGLE conferees on the part of the Senate.

PROVIDING FOR A TEMPORARY EXTENSION OF THE INTERSTATE TRANSFER DEADLINE FOR THE H-3 HIGHWAY

Mr. BYRD. Mr. President, on behalf of Mr. INOUYE, I ask unanimous consent that S. 2900, which is at the desk, be called up and that the Senate proceed to its immediate consideration.

The PRESIDING OFFICER. The clerk will report.

The assistant legislative clerk read as follows:

A bill (S. 2900) to provide a temporary extension of the interstate transfer deadline for the H-3 highway

The PRESIDING OFFICER. Without objection the Senate will proceed to its immediate consideration.

The Senate proceeded to consider the bill.

The PRESIDING OFFICER. The bill is before the Senate and open to