matics, the sciences, communications skills, foreign languages, and technology; and

(2) where necessary, for guidance and counseling.

(b) PERMISSIBLE USES OF REFORM AND EQUITY FUNDS.—(1) Funds retained by a State pursuant to section 5(b)(1) may be used to administer and carry out categorical programs and projects.

(2) Funds allocated to any local educational agency pursuant to section 5(b)(2) may be used for the development, expansion, or improvement of any of the following categorical programs and projects:

(A) early childhood education;

(B) school day care;

(C) in-service teacher training;

(D) dropout prevention;

(E) effective schools; and

(F) improvement of secondary schools basic skills instruction.

SEC. 7. APPLICATION REQUIREMENTS.

(a) STATE APPLICATION.—In order to receive an allocation under section 4 or 5 for any fiscal year, each State shall submit an application to the Secretary that—

(1) meets the requirements of paragraphs (1), (2), (3), (5), (6), and (8) of section 435(b) of the General Education Provisions Act (20 U.S.C. 1232d(b)); and

(2) describes the intended use of funds to be retained by the State under section 5 to enhance State reform efforts.

(b) SUBMISSION OF LOCAL APPLICATIONS FOR GENERAL EXCELLENCE AND REFORM AND EQUITY FUNDS.—(1) For any fiscal year, a local educational agency may submit a single application for an allocation under section 4 or an allocation under section 5, or both. Two or more local educational agencies that propose to conduct joint programs and projects from funds provided under section 4 may file such application as a consortium or other combination.

(2) A local educational agency may not apply for an allocation under section 5 unless the total number of children aged 5 to 17, inclusive, in the schools of such agency who are eligible to be counted under section 111(c) of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 2711(c)) exceeds the lesser of 5,000 or 20 percent of the total enrollment of such schools.

(c) CONTENTS OF LOCAL APPLICATIONS.—(1) In order to receive an allocation under section 4(b)(2) or under section 5(b)(2) for any fiscal year, a local educational agency shall have on file with the State educational agency an application which describes the programs and projects to be conducted with such allocation and which includes a plan for the improvement of the selected educational areas covered by such programs and projects.

(2) An application by a local educational agency or consortium thereof, or renewal of such an application, shall also contain assurances that—

(A) the programs and projects are designed and implemented in consultation with parents and classroom teachers of the children to be served;

(B) the funds received under this Act will be used only so as to supplement and, to the extent practical, increase the level of funds that would, in the absence of funds received under this Act, be available from non-Federal sources for the education of pupils participating in programs and projects assisted under this Act, and in no case used so as to supplant funds from such non-Federal sources; and

(C) the local educational agency will comply with the requirements of subsection (d), relating to maintenance of effort.

(d) MAINTENANCE OF EFFORT.—(1) Except as provided in paragraph (2), a local educational agency may receive funds under this Act for any fiscal year only if the State educational agency finds that either the combined fiscal effort per student or the aggregate expenditures of that agency and the State with respect to the provision of free public education by that agency for the preceding fiscal year was not less than 90 percent of such combined fiscal effort or aggregate expenditures for the second preceding fiscal year.

(2) The State educational agency shall reduce the amount of the allocation of funds under this Act in any fiscal year in the exact proportion to which a local educational agency fails to meet the requirement of paragraph (1) by falling below 90 percent of both the combined fiscal effort per student and aggregate expenditures (using the measure most favorable to such local agency), and no such lesser amount shall be used for computing the effort required under paragraph (1) for subsequent years.

(3) The State educational agency may waive, for one fiscal year only, the requirements of this subsection if the State educational agency determines that such a waiver would be equitable due to exceptional or uncontrollable circumstances such as a natural disaster or a precipitous and unforeseen decline in the financial resources of the local educational agency.

SEC. 8. EDUCATIONAL ACCOUNTABILITY.

(a) ACCOUNTABILITY FOR USE OF FUNDS.—(1) Each local educational agency receiving an allocation under this Act for any fiscal year shall submit to the State educational agency—

(A) evidence of progress in particular areas for which funds were expended; or

(B) evidence of general improvement in the educational system, such as—

(i) reductions in, or the maintenance of acceptable levels of, absenteeism, discipline problems (such as suspension and expulsion), and dropouts at the secondary level;

(ii) more instructional time; and

(iii) smaller class size.

(2) At the State's discretion, the State educational agency may conduct audits on a sampling basis to verify the accuracy of the local educational agency submissions under this subsection.

(b) CONTINUED FUNDING CONTINGENT ON PROGRESS DEMONSTRATION.—No local educational agency shall be eligible to obtain an allocation under this Act for more than three fiscal years unless the evidence submitted under subsection (a) demonstrates progress as verified by the State.

SEC. 9. BUSINESS INVOLVEMENT MATCHING GRANTS.

From the amount reserved for purposes of this section pursuant to the second sentence of section 5(a), the Secretary is authorized to make grants to local educational agencies in an amount equal to not more than 50 percent of the fair market value of any donations made to such agency by local business concerns for the conduct of programs and projects under this Act. Such donations may be in cash or in kind, and may consist of equipment, the services of business personnel, or training provided to such agency.

SEC. 10. DEFINITIONS.

As used in this Act, the term—

(1) "Secretary" means the Secretary of Education;

(2) "State" means the several States, the District of Columbia, and Puerto Rico, and, except for purposes of sections 4(a) and 5(a), includes Guam, American Samoa, the Virgin Islands, the Northern Mariana Islands, and the Trust Territory of the Pacific Islands;

(3) "State educational agency" has the meaning provided by section 595(a)(3) of the Education Consolidation and Improvement Act of 1981;

(4) "local educational agency" has the meaning provided by section 595(a)(4) of such Act;

(5) "parent" has the meaning provided by section 595(a)(5) of such Act; and

(6) "elementary school" and "secondary school" have the meaning provided by section 595(a)(7) of such Act.●

By Mr. LEAHY (for himself and Mr. MATHIAS):

S. 1667. A bill to amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes; to the Committee on the Judiciary.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

Mr. LEAHY. Mr. President, for years this body has talked about the potential loss of personal privacy which could result from the electronic revolution. Today, I am introducing the Electronic Communications Privacy Act of 1985 which aims at ending the talk and beginning the process of ensuring the privacy of communications of individual Americans and American businesses. I am very pleased to be joined in this effort by my distinguished colleague from Maryland, Senator MATHIAS.

Let me describe a problem that grows as we sit here.

At this moment phones are ringing, and when they are answered, the message that comes out is a stream of sounds denoting one's and zero's. Nothing more. I am talking about the stream of information transmitted in digitized form, and my description covers everything from interbank orders to private electronic mail hookups.

By now this technology is nothing remarkable. What is remarkable is the fact that none of these transmissions are protected from illegal wiretaps, because our primary law, passed back in 1968, failed to cover data communications, of which computer-to-computer transmissions are a good example.

When Congress enacted that law, title III of the Omnibus Crime Control and Safe Streets Act of 1968, it had in mind a particular kind of communication—voice—and a particular way of transmitting that communication—via a common carrier analog telephone network. Congress chose to cover only the "aural acquisition" of the contents of a common carrier wire communication. The Supreme Court has interpreted that language to mean that to be covered by title III, a communica-

tion must be capable of being overheard. The statute simply fails to cover the unauthorized interception of data transmissions.

Similarly, there is no adequate Federal legal protection against the unauthorized access of electronic communications system computers to obtain or alter the communications contained in those computers.

Problems also exist with regard to the legal protection afforded to cellular radio telephones, electronic pagers, and the private transmissions of video signals such as that used in teleconferencing.

There may have been a day when good locks on the door and physical control of your own papers guaranteed a certain degree of privacy.

But the new information technologies have changed all that.

Hearings in the last Congress held by Senator MATHIAS and myself in the Senate Judiciary Committee and by Congressman ROBERT KASTENMEIER in the House Judiciary Committee clearly demonstrate the scope of these problems and the need to act.

Congressman KASTENMEIER, Senator MATHIAS, and I have been working for over a year with the Justice Department and many individuals, businesses, and industry groups who are concerned with updating the law to better protect communications privacy.

The product of that effort is the bill which Senator MATHIAS and I are introducing today. Congressman KASTENMEIER and Congressman MOORHEAD are introducing identical legislation in the House.

The Electronic Communications Privacy Act of 1985 contains a number of important changes:

The act amends title III of the Omnibus Crime Control and Safe Streets, Act of 1968—the Federal wiretap law.

Definitions contained in title III are amended to broaden protection from only voice transmissions to all electronic communications including data and video carried on nonpublic systems. The requirement that to fall within the coverage of title III an interception has to be by "aural acquisition," is dropped.

Protection of only common carrier telephone systems is broadened to include all electronic communications systems unless designed to be accessible by the public.

The bill contains criminal penalties for unauthorized access to the computers of an electronic communication system, if messages contained therein are obtained or altered. If done for commercial gain or for malicious reasons, the crime could be prosecuted as a felony offense.

To obtain communications contained in the computers of an electronic communication system, such as an electronic mail service, the Government would be required to obtain a warrant based on a probable cause standard.

An operator of an electronic communications system is restricted from disclosing the contents of an electronic message except in specified circumstances or unless authorized by the person sending the message.

An electronic communications system and the users of the system are granted a Federal cause of action to seek civil damages for violation of any of the rights contained in the act.

Finally, the bill provides that law enforcement agencies must obtain a court order based on a reasonable suspicion standard before installing a pen register or being permitted access to records of an electronic communications system which concern specific communications.

The bill does not affect the carefully balanced provisions governing foreign intelligence surveillance contained in the Foreign Intelligence Surveillance Act of 1978.

These changes will go a long way toward providing the legal protections of privacy and security which the new communications technologies need to flourish.

As I said earlier, we have worked hard over the past year to listen to all affected interests and to accommodate the legitimate needs of law enforcement while securing the privacy rights of users and operators of electronic communications systems.

A number of tough questions remain to be answered. Chief amongst these is whether electronic communications systems which are not designed to protect the privacy of the communications being carried should be afforded legal protection.

But raising this question should in no way suggest that communications privacy is just an industry problem.

It is no solution to say that anybody concerned about the privacy of these communications can pay for security by paying for encryption.

Encryption can be broken. But more importantly, the law must protect private communications from interception by an eavesdropper, whether the eavesdropper is a corporate spy, a police officer without probable cause, or just a plain snoop.

Unauthorized acquisition of information is not just a theoretical problem, or one confined to harmless teenage hackers. Communications companies have been faced with Government demands, unaccompanied by a warrant for access to the message contained in electronic mail systems. And the unwanted private intruder, whether a competitor or a malicious teenager, can do a great deal of damage before being, or without being, discovered.

From the beginning of our history, first-class mail has had the reputation for preserving privacy, while at the same time promoting commerce.

Both of these important interests must continue into our new information age. We cannot let any American feel less confident in putting information into an electronic mail network than he or she would in putting it into an envelope and dropping it off at the Post Office.

Thomas Jefferson once observed that—

> Laws and institutions must go hand-in-hand with the progress of the human mind. . . . As new discoveries are made . . . institutions must advance also, and keep pace with the times.

American businesses have produced a marvelous array of possibilities for better and faster communication worldwide. Now is the time for our legal institutions to also advance and keep pace with the times.

The protection of communications privacy can go hand-in-hand with progress. Our job is to make both a reality. Now is the time to act.

I ask unanimous consent that a summary of the bill and its text be printed in the RECORD at this point.

There being no objection, the materials were ordered to be printed in the RECORD, as follows:

S. 1667

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 "Electronic Communications Privacy Act of 1985".

TITLE I—TITLE 18 AND RELATED MATTERS

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

(a) DEFINITIONS.—(1) Section 2510 of title 18, United States Code, is amended by striking out paragraph (1) and inserting in lieu thereof the following:

"(1) 'electronic communication' means any transmission of signs, signals, writing, images, sounds, data, or intelligence of any *nature in whole or in part by a wire, radio,* electromagnetic, or photoelectric system that affects interstate or foreign commerce;".

(2) Section 2510(4) of title 18, United States Code, is amended by striking out "aural acquisition" and inserting "interception" in lieu thereof.

(3) Section 2510(8) of title 18, United States Code, is amended by striking out "existence,".

(b) EXCEPTIONS WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—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 for any person—

"(i) to intercept an electronic communication made through an electronic communication system designed so that such electronic communication is readily accessible to the public.

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

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

"(II) by a walkie talkie, or a police or fire communication system readily accessible to the public; or

"(III) by an amateur radio station operator or by a citizens band radio operator; or

"(iii) to engage in any conduct which—

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

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

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

"(i) to use a pen register (as that term is defined for the purposes of chapter 206 (relating to pen registers) of this title); or

"(ii) for a provider of electronic communication service to record the placement of a telephone call in order to protect such provider, or a user of that service, from abuse of service.".

(c) TECHNICAL AND CONFORMING AMENDMENTS.—(1) Chapter 119 of title 18, United States Code, is amended by striking out "wire" each place it appears (including in any section heading) and inserting "electronic" in lieu thereof.

(2) The heading of chapter 119 of title 18, United States Code, is amended by inserting "AND OTHER ELECTRONIC COMMUNICATION" 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 other electronic communication" after "wire".

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

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

(B) by striking out "of the carrier" 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 electronic communication service" in lieu thereof.

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

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

(B) by striking out "communications common carrier" each place it appears and inserting "provider of electronic communication services" in lieu thereof.

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

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

SEC. 102. ADDITIONAL PROHIBITIONS RELATING TO ELECTRONIC COMMUNICATIONS AND REQUIREMENTS FOR CERTAIN DISCLOSURES.

(a) ADDITIONAL PROHIBITIONS.—Section 2511 of title 18, United States Code, is amended by adding at the end the following:

"(3) Unless authorized by the person or entity providing an electronic communication service or by a user of that service, and except as otherwise authorized in section 2516 of this title, whoever willfully accesses an electronic communication system through which such service is provided or willfully exceeds an authorization to access that electronic communication service and obtains or alters that electronic communication while it is stored in such system shall—

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

"(i) be fined not more than $250,000 or imprisoned not more than one year, or both, in the case of a first offense under this subparagraph; and

"(ii) be fined not more than $250,000 or imprisoned not more than two years, or both, for any subsequent offense under this subparagraph; and

"(B) be fined not more than $5,000 or imprisoned not more than six months, or both, in any other case.

"(4) A person or entity providing an electronic communication service shall not knowingly divulge the contents of any communication (other than one to such person or entity) carried on that service to any person or entity other than the addressee of such communication or that addressee's agent, except—

"(A) as otherwise authorized in section 2516 of this title;

"(B) with the consent of the user originating such communication;

"(C) to a person employed to forward such communication to its destination; or

"(D) for a business activity related to a service provided by the provider of the electronic communication service to a user of the electronic communication service.".

(b) REQUIREMENTS FOR CERTAIN DISCLOSURES.—(1) Section 2516 of title 18, United States Code, is amended by adding at the end the following:

"(3) a person authorized to make application under this section for an interception may also make an application for a disclosure which would otherwise be in violation of section 2511(3) or (4). Such application shall meet the requirements for an application for an interception under this section. The court shall not grant such disclosure unless the applicant demonstrates that the particular communications to be disclosed concern a particular offense enumerated in section 2516 of this title. If an order of disclosure is granted, disclosure of information under that order shall not be subject to the prohibitions contained in such section 2511(3) or (4). Such disclosure shall be treated for the purposes of this chapter as interceptions under this chapter, and shall be subject to the same requirements and procedures as apply under this chapter to interceptions under this chapter.

"(4) A provider of electronic communication service may not, upon the request of a governmental authority, disclose to that authority a record kept by that provider in the course of providing that communication service and relating to a particular communication made through that service, unless the governmental authority obtains a court order for such disclosure based on a finding that—

"(A) the governmental entity reasonably suspects the person or entity by whom or to whom such communication was made to have engaged or to be about to engage in criminal conduct; and

"(B) the record may contain information relevant to that conduct.

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) Any person whose electronic communication or oral communication is intercepted, accessed, disclosed, or 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) 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

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

"(c) The court may assess as damages in an action under this section either—

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

"(2) statutory damages in an amount not less than $500 or more than $10,000.

"(d) A good faith reliance on a court warrant or order is a complete defense against a civil action under this section.

"(e) A civil action under this section may not be commenced later than two years after whichever is later of—

"(1) the date of the occurrence of the violation; or

"(2) the date upon which the claimant first has had a reasonable opportunity to discover the violation.".

SEC. 104. CERTAIN APPROVALS BY ACTING ASSISTANT ATTORNEY GENERAL.

Section 2516(1) of title 18 of the United States Code is amended by inserting "(or acting Assistant Attorney General)" after "Assistant Attorney General".

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

Section 2516(1)(c) of title 18 of the United States Code is amended—

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

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

(3) 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 32 (relating to destruction of aircraft or aircraft facilities)," after "stolen property),"; and

(4) 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),".

SEC. 106. ADDITIONAL REQUIREMENTS FOR APPLICATIONS, ORDERS, AND IMPLEMENTATION OF ORDERS.

(a) INVESTIGATION OBJECTIVES.—Section 2518(1)(b) of title 18 of the United States Code is amended by inserting immediately before the semicolon at the end the following: ", and (v) the specific investigative objectives and the specific targets, if known, of the interception to which the application pertains".

(b) ALTERNATE INVESTIGATIVE TECHNIQUES.—Section 2518(1)(c) of title 18 of the United States Code is amended by inserting "(including the use of consensual monitoring, pen registers, tracking devices, contempt proceedings, perjury prosecutions, use of accomplice testimony, grand jury sub-

poena of documents, search warrants, interviewing witnesses, and obtaining documents through other legal means)" after "procedures".

(c) 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 installed within such jurisdiction)" after "within the territorial jurisdiction of the court in which the judge is sitting".

(d) REIMBURSEMENT FOR ASSISTANCE; PHYSICAL ENTRY.—Section 2518(4) of title 18 of the United States Code is amended—

(1) by striking out "at the prevailing rates" and inserting in lieu thereof "for reasonable expenses incurred in providing such facilities or assistance"; and

(2) by adding at the end "An order authorizing the interception of an electronic communication under this chapter may, upon a showing by the applicant that there are no other less intrusive means reasonably available of effecting the interception, authorize physical entry by law enforcement officers to install an electronic, mechanical, or other device. No such order may require the participation of any individuals operating or employed by an electronic communications system in such physical entry.".

(e) PERIODIC REPORTS.—Subsection (6) of section 2518 of title 18 of the United States Code is amended to read as follows:

"(6) An order authorizing interception pursuant to this chapter shall require that reports be made not less often than every ten days to the judge who issued such order, showing what progress has been made toward achievement of the authorized objective, the need, if any for continued interception, and whether any evidence has been discovered through such interception of offenses other than those with respect to which such order was issued. The judge may suspend or terminate interception if any such report is deficient or evinces serious procedural irregularities. The judge shall terminate interception if the legal basis of continued interception no longer exists.".

(f) TIME LIMIT FOR THE MAKING AVAILABLE TO JUDGE OF RECORDINGS.—Section 2518(8)(a) of title 18 of the United States Code is amended by striking out "Immediately upon" and inserting "Not later than 48 hours after" in lieu thereof.

SEC. 107. EFFECTIVE DATE.

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.

TITLE II—PEN REGISTERS AND TRACKING DEVICES

SEC. 201. 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 TRACKING DEVICES

"Sec.

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

"(a) IN GENERAL.—Except as provided in this section or section 3124 of this title, no person may install or use a pen register or a tracking 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 by a provider of electronic communication services relating to the operation, maintenance, and testing of an electronic communication service.

"(c) PENALTY.—Whoever knowingly violates subsection (a) shall be fined not more than $100,000 or imprisoned not more than one year, or both.

"§ 3122. Application for an order for a pen register or tracking device

"(a) LAW ENFORCEMENT OFFICERS MAY MAKE APPLICATION.—(1) A Federal law enforcement officer having responsibility for an ongoing criminal investigation 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 tracking device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

"(2) A State law enforcement officer having responsibility for an ongoing criminal investigation 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 tracking 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 law enforcement officer making the application and of any other officer or employee authorizing or directing such application, and the identity of the agency in which each such law enforcement officer and other officer or employee is employed; and

"(2) a statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that an order should be issued.

"§ 3123. Issuance of an order for a pen register or tracking device.

"(a) IN GENERAL.—Upon an application made under section 3122 of this title, the court may enter an ex parte order, as requested or as found warranted by the court, authorizing or approving the installation and use of a pen register or a tracking device within the jurisdiction of the court (and outside that jurisdiction but within the United States in the case of a mobile tracking device installed within such jurisdiction) if the court finds on the basis of the information submitted by the applicant that—

"(1) in the case of a pen register, there is reasonable cause to believe; and

"(2) in the case of a tracking device, there is probable cause to believe;

that the information likely to be obtained by such installation and use is relevant to a legitimate 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, in whose name is listed, or who commonly uses the telephone line to which the pen register is to be attached or of the person to be traced by means of the tracking device;

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

"(C) the number of the telephone line to which the pen register is to be attached, or the identity of the object to which the tracking device is to be attached;

"(D) a statement of the nature of the criminal investigation to which the information likely to be obtained by the pen register or tracking device relates;

"(E) the identity of the law enforcement officer authorized to install and use the pen register or tracking device; and

"(F) the period of time during which the use of the pen register or tracking device is authorized; and

"(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation and use of the pen register or tracking device under section 3125 of this title.

"(c) TIME PERIOD AND EXTENSIONS.—(1) An order issued under this section may authorize or approve the installation and use of a pen register or tracking device for the period necessary to achieve the objective of the authorization, or for 30 days, whichever is less.

"(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 extension shall include a full and complete statement of any changes in the information required by subsection (b) of this section to be set forth in the original order. The period of extension may be for the period necessary to achieve the objective for which it was granted, or for 30 days, whichever is less.

"(d) NONDISCLOSURE OF EXISTENCE OF PEN REGISTER OR TRACKING DEVICE.—An order authorizing or approving the installation and use of a pen register or tracking device shall direct that the person owning or leasing the line to which the pen register is attached, or who has been ordered by the court to provide assistance to the applicant, shall not disclose the existence of the pen register or tracking device until at least 60 days after its removal. Upon the request of the applicant, the court may order such person to postpone any disclosure of the existence of the pen register or tracking device for additional periods of not more than 60 days each, if the court finds, upon the showing of the applicant, that there is reason for the belief that disclosing the existence of the pen register or tracking device may—

"(1) endanger the life or physical safety of any person;

"(2) result in flight from prosecution;

"(3) result in destruction of, or tampering with, evidence;

"(4) result in intimidation of potential witnesses; or

"(5) otherwise seriously jeopardize an investigation or governmental proceeding.

"§ 3124. Emergency use of pen register or tracking device without prior authorization

"(a) IN GENERAL.—A law enforcement officer specially designated by the Attorney General may install and use a pen register or a tracking device without a court order, if a judge of competent jurisdiction is notified at the time the decision to make such installation and use is made, and if—

"(1) such law enforcement officer reasonably determines that—

"(A) an emergency situation exists that involves—

"(i) immediate danger of death or serious bodily injury to any person;

"(ii) conspiratorial activities threatening the national security interest; or

"(iii) conspiratorial activities characteristic of organized crime; that requires the installation and use of a pen register or a tracking device before an order authorizing the installation and use of the pen register or tracking device can, with due diligence, be obtained; and

"(B) there are grounds upon which an order could be entered under section 3123 of this title to authorize the installation and use of such pen register or tracking device; and

"(2) an application for an order approving the installation and use of the pen register or tracking device is made under section 3122 of this title as soon as practicable but not more than 48 hours after the pen register or tracking device is installed.

"(b) TERMINATION.—In the absence of an order approving the pen register or tracking device, the use of the pen register or tracking device shall terminate immediately when the information sought is obtained, or when the application for the order is denied, whichever is earlier.

"§3125. Assistance in installation and use of a pen register or tracking device

"(a) IN GENERAL.—Except as provided in subsection (b), upon the request of a law enforcement officer authorized by this chapter to install and use a pen register or tracking device, a communications common carrier, landlord, custodian, or other person shall furnish such law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation and use of the pen register or tracking 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—

"(1) such assistance is directed by a court order as provided in section 3123(b)(2) of this title; or

"(2) the emergency installation and use of the pen register or tracking device is authorized under section 3124 of this title.

"(b) EXCEPTION.—A law enforcement officer may not request the participation under this section of any individuals operating or employed by an electronic communications system in such physical entry.

"(c) COMPENSATION.—A communications common carrier, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be compensated for such assistance for reasonable expenses incurred in providing such facilities or assistance.

"§ 3126. Notice to affected persons

"(a) SERVICE OF INVENTORY.—Except as provided in subsection (b), within a reasonable time but not later than ninety days after the filing of an application for an order of approval required under section 3124 of this title, if such application is denied, or the termination of an order, as extended, under section 3123 of this title, the issuing or denying judge shall cause to be served on the persons named in the order or application, and such other parties to activity monitored by means of a pen register or tracking device as the judge may determine in the judge's discretion that it is in the interest of justice, an inventory which shall include notice of—

"(1) the fact of the entry of the order or the application;

"(2) the date of such entry and the period of authorized, approved, or disapproved activity under such order, or the denial of the application; and

"(3) the fact that during the period activity took place under such order.

"(b) EXCEPTION.—On an ex parte showing of good cause to a judge of competent jurisdiction—

"(1) the serving of the inventory required by this subsection may be postponed; and

"(2) the serving of such inventory may be dispensed with if notice under this section would compromise an ongoing criminal investigation or result in the disclosure of classified information harmful to the national security.

"(c) MOTION FOR INSPECTION.—The judge, upon the filing of a motion, may in the judge's discretion make available to such person or such person's counsel for inspection such portions of the results of activity under such order or referred to in such application, and such orders and applications as the judge determines to be in the interest of justice.

"§ 3127. Reports concerning pen registers and tracking devices

"(a) REPORT BY ISSUING OR DENYING JUDGE.—Within thirty days after the expiration of an order (or each extension thereof) entered under section 3123 of this title, or the denial of an order approving the use of a pen register or a tracking device, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

"(1) the fact that an order or extension applied for;

"(2) the kind of order or extension applied for;

"(3) the fact that the order or extension was granted as applied for, was modified, or was denied;

"(4) the period of operation of the pen register or tracking device authorized by the order, and the number and duration of any extensions of the order;

"(5) the offense specified in the order or application, or extension of an order;

"(6) the identity of the applying law enforcement officer and agency making the application and the person authorizing the application; and

"(7) the nature of the facilities from which or the place where activity under the order was to be carried out.

"(b) REPORT BY ATTORNEY GENERAL.—In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Officer of the United States Courts—

"(1) the information required by paragraphs (1) through (7) of subsection (a) of this section with respect to each application for an order or extension made during the preceding calendar year;

"(2) a general description of the pen registers and tracking devices conducted under such order or extension, including—

"(A) the approximate nature and frequency of incriminating evidence obtained;

"(B) the approximate number of persons whose activities were monitored; and

"(C) the approximate nature, amount, and cost of the manpower and other resources used in carrying out orders under this chapter;

"(3) the number of arrests resulting from activity conducted under such order or extension, and the offenses for which arrests were made;

"(4) the number of trials resulting from such activity;

"(5) the number of motions to suppress made with respect to such activity, and the number granted or denied;

"(6) the number of convictions resulting from such activity and the offenses for which the convictions were obtained and a general assessment of the importance of such activity; and

"(7) the information required by paragraphs (2) through (6) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

"(c) REPORT BY DIRECTOR OF ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS.—In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders under this chapter and the number of orders and extensions granted or denied under this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (a) and (b) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (a) and (b) of this section.

"§ 3128. Recovery of civil damages authorized

"(a) Any person who is harmed by a 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) In an action under this section, appropriate relief includes—

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

"(2) damages; and

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

"(c) A good faith reliance on a court warrant or order is a complete defense against a civil action under this section.

"(d) A civil action under this section may not be commenced later than two years after whichever is later of—

"(1) the date of the occurrence of the violation; or

"(2) the date upon which the claimant first has had a reasonable opportunity to discover the violation.".

"§ 3129. Definitions for chapter

"As used in this chapter—

"(1) the term 'communications common carrier' has the meaning set forth for the term 'common carrier' in section 3(h) of the Communications Act of 1934 (47 U.S.C. 153(h));

"(2) the term 'electronic communication' has the meaning set forth for such term in section 2510 of this title;

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

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

"(B) a court of general criminal jurisdiction of a State authorized by a statute of that State to enter orders authorizing the use of pen registers and tracking devices in accordance with this chapter;

"(4) the term 'legitimate criminal investigation' means a lawful investigation or official proceeding inquiring into a violation of any Federal criminal law;

"(5) the term 'pen register' means a device which records and 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 of electronic communication services for billing, or recording as an incident to billing, for communications services provided by such provider;

"(6) the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object in circumstances in which there exists a reasonable expectation of privacy with respect to such tracking; and

"(7) 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 Tracking Devices 3121

SEC. 202. EFFECTIVE DATE.

This title and the amendments made by this title shall take effect on the date of the enactment of this Act.

SUMMARY OF THE BILL

There are seven major features of the bill:

1. The bill extends the protection against interception from voice transmissions to virtually all electronic communications. Thus, legal protection will be extended to the digitized portion of telephone calls, the transmission of data over telephone lines, the transmission of video images by microwave, or any other conceivable mix of medium and message. The bill also provides several clear exceptions to the bar on interception so as to leave unaffected electronic communication made through an electronic communication system designed so that such communication is readily available to the public (e.g., walkie talkies, police or fire communications systems, ship-to-shore radio, ham radio operators or CB operators are not affected by the bill).

2. The bill eliminates the distinction between common carriers and private carriers, because they each perform so many of the same functions. The size of many of the private carriers makes them appropriate for inclusion within the protection of federal laws.

3. The bill creates criminal and civil penalties for persons who—without judicial authorization—obtain access to an electronic communication system and obtain or alter information. This provision parallels that dealing with interception (see #1, above). It would be inconsistent to prohibit the interception of digitized information while in transit and leave unprotected the accessing of such information while it is being stored. This part of the bill assures consistency in this regard.

4. The bill protects against the unauthorized disclosure of third party records being held by an electronic communication system. Without such protection the carriers of such messages would be free to disclose records of private communications to the government without a court order. Thus, the bill provides that a governmental entity must obtain a court order under appropriate standards before it is permitted to obtain access to these records. This requirement, while protecting the government's legitimate law enforcement needs, will serve to minimize intrusiveness for both system users and service providers. This provision also assures that users of a system will have the right to contest allegedly unlawful government actions. The approach taken in the bill is similar to the Congressional reaction to the Supreme Court decision in *United States* v. *Miller*, 425 U.S. 435 (1976), when we enacted the Right to Financial Privacy Act of 1978, 12 U.S.C. 3401 et seq.

5. The interests of law enforcement are enhanced by updating the provisions of Federal law relating to wiretapping and bugging. Under current law an Assistant Attorney General must personally approve each interception application. The bill permits an Acting Assistant Attorney General to approve such applications. The bill also expands the list of crimes for which a tap or bug order may be obtained to include the crimes of escape, chop shop operation, murder for hire, and violent crimes in aid of racketeering.

6. The basic provisions of the Federal wiretapping law are updated to: (1) require that the application for a court-ordered tap or bug disclose to the court the investigative objective to be achieved; (2) the application must indicate the viability of alternative investigative techniques; (3) authorizes the placement of certain mobile interception devices; (4) authorizes physical entry into the premises to install the bug or tap conistent with *Dalia* v. *United States*, 441 U.S. 238 (1979); and (5) rationalizes the government's reporting obligations after a tap or bug has been obtained.

7. The bill regulates the government use of pen registers and tracking devices. Pen registers are devices used for recording which phone numbers have been dialed from a particular phone. Tracking devices are devices which permit the tracking of the movement of a person or object in circumstances where there exists reasonable expectation of privacy. Tracking devices, therefore, include "beepers" and other nonphone surveillance devices.

The bill requires the government to obtain a court order based upon "reasonable cause" before it can use a "pen register." This standard resembles current administrative practice. *Compare United States* v. *New York Telephone Co.*, 434 U.S. 159 (1977) (a title III order is not required for pen registers); *Smith* v. *Maryland*, 442 U.S. 735 (1979) (pen registers not regulated by the Fourth Amendment). The bill requires that the government show probable cause to obtain a court order for a tracking device. This showing is consistent with the current law. *United States* v. *Karo*, 104 S. Ct. 3296 (1984).

Mr. MATHIAS. Mr. President, I am pleased to join today with the distinguished junior Senator from Vermont [Mr. LEAHY] to introduce the Electronic Communications Privacy Act of 1985. With the drafting of this legislation, we take an important step in the process of bringing our laws up to date with modern technology. This bill addresses itself to forms of electronic communication that are new and unusual to many Americans. But the goal of the legislation is a familiar and enduring one: To protect the privacy of Americans against unwanted and unwarranted intrusion.

The stimulus for this legislation was a hearing held in the Subcommittee on Patents, Copyrights and Trademarks last year, on the topic of communications privacy. But its genesis really goes back much further in our history. More than half a century ago, Justice Louis Brandeis sounded an eloquent warning about the challenge to privacy posed by technological advances. In his famous dissent in the wiretapping case of Olmstead versus United States, Brandeis emphasized that if the right to privacy is to be meaningful, it must be strong enough to meet this challenge. As he put it:

> The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping. Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.

That prospect must have appeared fanciful to most of Brandeis' contemporaries. But we know better. Brandeis' "someday" has arrived, and the law must respond.

Technological wizardry offers a variety of new communications media: electronic mail, the cellular telephone, local area networks, computer-to-computer data transmissions, and many more. Individuals and businesses are taking advantage of these new ways to share information of every kind and description.

Some of the messages that these new media carry are highly sensitive. A translation of the digital bits that race across our country by wire, microwave, fiber optics and other paths could reveal proprietary corporate data, or personal medical or financial information. The users of these networks—and that means more and more of us—expect and deserve legal protection against unwarranted interceptions of this data stream, whether by overzealous law enforcement officers or private snoops.

The laws on the books today may not provide that protection. The major statutory bulwark against one form of data interception—wiretapping—forbids only the unauthorized "aural acquisition" of wire communications. This definition does not fully encompass the complex web of transmission media that have become the nervous system of our economy and our society. Nor does it explicitly protect the growing volume of messages that cannot be acquired "aurally" because, even though they may be in-

tended as confidential, they never take the form of the spoken word. Clearly, Brandeis' warning must be heeded; the law must be brought up to date with the progress of science.

The Electronic Communications Privacy Act responds to that challenge in several ways. It plugs the loopholes in the 1968 wiretap statute by forbidding the unauthorized interception of private electronic communications of any description. It provides legal protection for messages in electronic communication systems, not only while they are in the stream of transmission, but even after they have come to rest, by forbidding—with certain exceptions—unauthorized access to and alteration of such messages. It clarifies the ground rules for disclosure of information about an individual's use of an electronic communications system—such as electronic mail—by requiring a court order before permitting the Government to obtain that information. The bill also seeks to codify the standards for law enforcement use of certain surveillance devices, including pen registers—which record the numbers dialed from a particular telephone—and tracking devices. Finally, the Electronic Communications Privacy Act makes other needed improvements in existing wiretap legislation to enhance judicial oversight of this essential law enforcement tool.

This is an ambitious and comprehensive piece of legislation that calls for careful examination. It is clear from the drafting process that has taken place thus far that this legislative foray into uncharted territory requires us to confront difficult legal and technical issues. The distinctions between communications media that are relatively accessible to the general public, and those as to which an expectation of privacy is justified and deserves legal recognition, must be drawn with as much precision as possible, and yet with enough flexibility to anticipate further technological developments. The relative obligations of individuals, communications service providers, law enforcement agencies, and the courts in the legal and technical protection of privacy must be carefully weighed. The need for, and the desirability of, the provisions on pen registers and tracking devices, must be critically examined. As we examine these and other aspects of the legislation, I look forward to working closely with the Justice Department, with the communications and computer experts in the private sector who have already contributed so much to the drafting of this legislation, and with my colleagues, to craft a statute that is comprehensive, clear, and appropriately responsive to the concerns of business and law enforcement.

In the months ahead, the Subcommittee on Patents, Copyrights and Trademarks, which has jurisdiction in the privacy sphere, will be examining this bill with care. Our efforts will be advanced immeasurably by the interest and initiative demonstrated by the ranking minority member of our subcommittee, Senator LEAHY, in introducing this bill today. I am also pleased to note that identical legislation is being introduced today in the House of Representatives by the chairman and ranking member of our counterpart subcommittee, Representatives ROBERT KASTENMEIER and CARLOS MOORHEAD.

I am confident that, through our cooperative efforts, we will be able to refine and improve this legislation, and thereby meet this new challenge to what Justice Brandeis referred to as "the most comprehensive of rights and the right most valued by civilized men," the right to privacy.

By Mr. CRANSTON (for himself and Mr. WILSON):

S. 1668. A bill imposing certain limitations and restrictions on leasing lands on the Outer Continental Shelf off the State of California, and for other purposes; to the Committee on Energy and Natural Resources.

CALIFORNIA OUTER CONTINENTAL SHELF PROTECTION AND DEVELOPMENT ACT

● Mr. CRANSTON. Mr. President, today along with my distinguished Republican colleague from California [PETE WILSON] I am introducing legislation that we believe will bring to an end in a sensible and balanced way the long-ranging debate over the Outer Continental Shelf off the coast of California. Similar legislation is also being introduced in the House, by a bipartisan group of 29 original cosponsors.

When the Reagan administration came to town, it claimed a mandate from what was called the Sagebrush Rebellion, the desire of sovereign States, especially Western States, to protect their rights free of the threat to those rights by bureaucracies of the central government, especially the Department of the Interior.

Unfortunately, the administration seems to have forgotten that mandate.

The administration seems perfectly willing to try to push around the California congressional delegation, using whatever leverage it can now muster.

That effort comes after the Secretary of the Interior has walked away from an agreement he negotiated with a bipartisan group of representatives of the California delegation in what he claimed and we understood to be good faith.

Those negotiations were a serious attempt to try to end the annual warfare over Federal OCS leasing that has plagued concerned citizens and the State, coastal county, and local governments of California since this administration took office and Secretary Watt attempted to lease the entire California coastline in a fire sale to the major oil companies.

A negotiated solution makes a great deal of sense, and is a course I have always tried to pursue since I became interested in this issue in 1969, 3 weeks after taking my Senate seat, when the very severe Santa Barbara oil blowout occurred, bringing the issue forcefully to my attention.

I have discussed California offshore leasing with eight different Secretaries of the Interior, seven of them Republicans. Only during the present administration have I become convinced that a legislative solution is needed to insure balanced protection to special portions of the California coastline.

As my colleagues know, for 4 consecutive years the full Congress has approved 1-year moratoriums, which included portions of the California coastline. In the past two Congresses I have introduced legislation, referred to the Committee on Energy and Natural Resources, to settle this issue. In the present Congress, that bill is S. 734. I am now introducing this bill which represents, with only very minor adjustments contemplated by the agreement itself, the preliminary agreement reached with Interior Secretary Don Hodel.

When the conference managers on the Interior appropriations bill agreed upon the moratorium language last year, they added language to the report which conditioned future moratoriums on failure of the negotiation process with the Department of the Interior to ensure adequate protection for all resource values and Department of Defense needs in specific areas, and urged the Department to pursue negotiations with the appropriate California congressional, State, and local officials.

Under such pressure, the Secretary did engage in negotiations with the interested members of the delegation—a careful, tough process which took place over a period of 6 weeks and through numerous sessions involving about 20 hours of close negotiations. Both California Senators participated in the process, and supported its outcome, an agreement in principle, struck and announced at a press conference just before the August recess in which the Secretary fully participated.

It was clear to all who participated that some minor further work needed to be done on a "national security clause" to the agreement, to craft an exception to cover the contingency of a new national energy emergency; that adjustment of the location of five tracts off Oceanside to locations nearer Camp Pendleton was desired—if the Department of Defense would concur, as I am informed that they now do—and that adjustment of the six tracts off Newport Beach (Orange