June 19, 1986

CONGRESSIONAL RECORD — SENATE S 7991

S. 2976. 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

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

Mr. LEAHY. Mr. President, I wish I could say that I am pleased to join my friend from Pennsylvania in sponsoring these two bills, but I cannot. The reason for my displeasure is that there should be no need for such legislation. If the proposed rule had only one role for the Federal Government after providing for the national defense, it should be disaster assistance to the States. But the Federal Emergency Management Agency—created to come to the rescue of the States in time of catastrophe—wants to cut drastically on the assistance it provides. That is shameful.

So, you see why I take no pleasure in sponsoring this legislation. It is introduced only to prevent FEMA from making a serious mistake. The Agency’s proposed rule would be devastating to Kentucky, Pennsylvania, Illinois, Indiana, Ohio, and Wisconsin. However, I also suspect it would be just as harmful to States of the Midwest and the Great Plains, which regularly are hit by tornados—California, which is hit by mudslides and brushfires every year—to the Gulf and Atlantic Coast States regularly lying in the path of hurricanes.

In fact, Mr. President, if the legislation we are introducing today is not signed into law before FEMA’s proposed rule becomes final, every State in the Union will run the risk of being unable to respond adequately if hit by a natural disaster. The Senate of Pennsylvania (Mr. Horszn), for recognizing the potential danger of FEMA’s rule, and for taking action to prevent it; and I hope my colleagues will join us in this effort.

Mr. LAUTENBERG. Mr. President, I am pleased to join today with my colleague from Pennsylvania, Senator Heinz, in introducing legislation to retain current Federal Emergency Management Agency policy on disaster relief.

In May, the Federal Emergency Management Agency issued draft regulations on disaster relief which, unless Congress intervenes, will become effective in October. The purpose of these regulations is to save FEMA money. The impact of the regulations is to make many communities suffering from disasters ineligible for Federal assistance.

Mr. President, of the last 111 Presidential declarations of disasters, only 61 would be eligible for assistance under the FEMA rules. Those found eligible for assistance would find themselves called upon to cover a far higher percentage of the cleanup and rehabilitation costs. FEMA would establish a scale of ability to pay based on per capita income. The fairness of such a sliding scale is worthy of debate and should, if it is to be implemented at all, be done legislatively and not by regulation.

To provide an example of the impact of these new regulations in New Jersey, I asked my State Office of Emergency Management to compare the cost to communities devastated by the 1984 spring floods. Passaic County, NJ had $1,664,000 in damages. After the Presidential declaration of disaster, the Federal Government paid 75/25 percent, matching $1,247,000 with the local share being $1,013,000, with FEMA covering $650,000.

Mr. President, historically, natural disasters have not been considered to be the fault of local communities and the Federal Government has attempted to quickly provide emergency relief. Until recently, the Federal Government covered 100 percent of disaster relief costs. In order to control costs, FEMA, without legislative mandate, began the 75/25 percent match with localities. That practice has not proven to be burdensome in most circumstances. Now it appears that FEMA wants to shift the burden of disaster relief primarily to States and localities.

Mr. President, the bill we are introducing will, for the first time, put in statute the 75/25 percent matching requirement. The bill will prevent FEMA from imposing, by regulation, the per capita scale which would rule States and localities ineligible for relief. The bill will prevent FEMA from adopting a 50/50 percent match.

Mr. President, as ranking minority member of the Environment and Public Works Committee’s Subcommittee on Regional and Community Development, I will be introducing my legislation on this issue. Disaster relief is one of the basic functions of Government. I strongly favor efforts to reduce unnecessary Federal spending, but I do not favor efforts to shift money at the expense of communities devastated by floods, hurricanes, coastal storms and other natural disasters.

I am pleased to be an original co-sponsor of this legislation and urge its swift consideration and adoption.

By Mr. LEAHY (for himself and Mr. MATHIAS):
somewhere in the United States right now.

Instead of the two business people discussing financial matters over the telephone, they use a video teleconference display to show their plans on their video screens. The same data is picked up by their competitor. Instead of going to the Post Office, the police officer goes to an electronic mail company. Ms. Doe is a user of the telephone, they use a video teleconferencing system and the officer asks to see all of Ms. Doe's messages.

The only real difference between the eavesdropper's and the policeman's system and the officer asks to see all the contents of others.

The Electronic Communications Privacy Act is designed to update our law to provide a reasonable level of Federal privacy protection to these new forms of communications. It is the culmination of 2 years of hard work. I want to commend the Senator from Maryland, the chairman of the Senate Judiciary Committee's Subcommittee on Patents, Copyrights and Trade-

I also want to congratulate Congresswoman CARLOS MOORHEAD, the chairman and ranking minority member of the House Judiciary Committee's Subcommittee on Courts, Civil Liberties and the Administration of Justice. The Congressmen and their staffs saw the House Judiciary Committee unanimously pass this landmark bill last week.

Mr. President, let me just briefly describe the limitations of current law and the development of this legislation. The Federal wiretap statute, title III of the Omnibus Crime and Safe Streets Act of 1968 is our primary law protecting the security and privacy of business and personal communications.

Eighteen years ago, when title III was written, Congress could not anticipate—or in some cases even contemplate—telecommunications and computer technology we are starting to take for granted today: electronic mail, computer-to-computer data transmissions, cellular telephones, paging devices, and video teleconferencing. Lawmakers in 1968 could not imagine the extensive use of communications and the exchange and processing of information which has put a wide range of personal and business records, including health, financial, and other records, "on line," or the types of electronic displays on their television screens, making it possible for overzealous law enforcement agencies, industrial spies, and just plain snoops to intercept the personal or proprietary communications of others.

Nor could Congress envision the dramatic developments 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. An ordinary telephone 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.

When Congress enacted title III, it had in mind one kind of communications—voice communications transmitted—a transmission via a common carrier analog—or regular voice—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 communication must be capable of being overheard.

Title III of the Omnibus Crime and Safe Streets Act is hopelessly out of date. It applies only to interceptions of voice communications transmitted via common carrier. It does not cover data communications. It does not specify whether or how communications made using electronic pagers or the private transmissions of video signals like those used in teleconferencing are protected.

Our 2-year effort to deal with this gap between the law and technological innovation began in 1984 when I asked the Attorney General whether he believed interceptions of electronic mail and computer communications were covered by the Federal wiretap laws.

The Criminal Division of the Department of Justice replied that Federal law protects electronic communications against unauthorized acquisitions only where a reasonable expectation of privacy exists. Undersecuring the need for this legislation, the Department concluded: "In this rapidly developing area of communications which range from cellular nonwire telephone connections to microwave-fed computer terminals, distinctions, such as whose—whether there does or does not exist a reasonable expectation of privacy—are not always clear or obvious."

Hearings in the 98th Congress by the Subcommittee on Patents, Copyrights and Trademarks and the House Judiciary Committee's Subcommittee on Courts, Civil Liberties, and the Administration of Justice have held extensive hearings on the legislation. During those hearings, the Department of Justice and radio hobbyists raised some concerns about the bill. Those concerns are addressed in this new version of the Electronic Communications Privacy Act. We are working with the Department of Justice and the House Judiciary Committee and by Congressman KASTENMEIER in the Senate Judiciary Committee and by Congressman KASTENMEIER in the House Judiciary Committee demonstrated the scope of these problems and the need to act. We began working with the Department of Justice and many individuals, businesses, industry carriers, and civil liberty groups. Those groups were concerned primarily about the need to update the law to better protect communications privacy. They also pointed out that the absence of such privacy protections may be inhibiting further technological development in this country.

The product of our discussions with the Department of Justice and these groups is a bill which will encourage the full use of modern computer technology available in America today.

During those discussions, two things became very clear. First, the need to address unauthorized acquisitions of information is very real. Communications companies have been faced with Government demands, unaccompanied by a warrant, for access to the messages 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 discovered—if he or she is ever discovered. Secret encryption is not the answer. It can be broken. More importantly, the law must protect private communications from interception by others.

The product of our discussions with the Department of Justice and these groups is a bill which will encourage the full use of modern computer technology available in America today.

Shortly thereafter, the Office of Technology Assessment issued its report, "Electronic Surveillance and Civil Liberties." Again, the need for this legislation was underlined. OTA concluded that a message sent by means of an electronic mail system could be intercepted and the contents disclosed to an unintended recipient. The Office of Technology Assessment study also concluded that current legal protections for electronic mail are "weakened or nonexistent," and that "electronic mail remains legally as well as technically vulnerable to unauthorized surveillance."

Since that time, the Subcommittee on Patents, Copyrights, and Trademarks and the House Judiciary Committee's Subcommittee on Courts, Civil Liberties, and the Administration of Justice have held extensive hearings on the legislation. During those hearings, the Department of Justice and radio hobbyists raised some concerns about the bill. Those concerns are addressed in this new version of the Electronic Communications Privacy Act. We are working with the Department of Justice and many individuals, businesses, industry carriers, and civil liberty groups. Those groups were concerned primarily about the need to update the law to better protect communications privacy. They also pointed out that the absence of such privacy protections may be inhibiting further technological development in this country. The enactment of such privacy protections will encourage the full use of modern computer technology available in America today.

The bill will extend coverage of title III of the Omnibus Crime and Safe Streets Act beyond only voice communications to include video and data communications. It recognizes that private carriers and common carriers
perform so many of the same func-
tions today that a distinction between
privacy standards is not warranted.
The bill also creates penalties for the
unauthorized use of electronically
stored information if that information
is obtained or altered.
In order to address radio hobbyists’
concerns, we modified the original lan-
guage of S. 1697 to clarify that inter-
cepting traditional radio services is not
unlawful. Under this revised Electroni-
c Communications Privacy bill, cellu-
lar phones, private and public micro-
waves, and any radio voice or display
are not.
The Electronic Communications Pri-
vacy Act provides standards by which
law enforcement agencies may obtain
access to both electronic communica-
tions and the records of an electronic
communications system. These provi-
sions are designed to protect legiti-
mate 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 Depart-
ment, we strengthened the current wire-
tap law from a law enforcement per-
spective. Specifically, we expanded the
list of felonies for which a voice wire-
tap is to be issued and the list of Justice
Department officials who may apply for a court order to
place a wiretap. We also added a provi-
sion making it easier for law enforce-
ment officials to deal with a target
who repeatedly changes telephones to
thwart interception of his communica-
tions, and created criminal penalties
for those who notify a target of a wire-
tap in order to obstruct it.
This is a statutory frame-
work for the authorization and issu-
ance of an order for a pen register.
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 em-
bedded in the Foreign Intelligence Sur-
veillance Act of 1978. And it provides
a clear procedure for access to telephone
toll records in counterintelligence in-
vestigations.
Mr. President, the subcommittee
staff has prepared a more detailed
summary of the bill. I ask unanimous
consent that the summary, along with
the text of the bill, be printed in the
Record following my remarks.
From the beginning of our history,
first-class mail has had the reputation
of preserving privacy while promoting
commerce. It is high time we updated
our laws so that we can say the same
about the forms of technology which
are being used by the side with first-
class mail. A broad coalition of busi-
nesses, industry groups, civil liberties
groups, and privacy groups are asking
us to do that by enacting the Electroni-
c Communications Privacy Act. The
Department of Justice also strongly
supports this legislation, and I look
forward to working with my colleagues
to see it passed and signed into law
this year.
In closing, let me just thank the
staff who have worked so hard, not
only in drafting a good bill, but in
working together until they success-
fully addressed the concerns raised
during the hearings. The bill now
enjoys the broadest possible support
and is ready for prompt passage in the
House and Senate, thanks to their ef-
forts.
There being no objection, the previ-
ously mentioned material was ordered
to be printed in the Record, as follows:
S. 3759
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 “Electro-
nic Communications Privacy Act of 1986”.
TITLE I—INTERCEPTION OF COMMU-
NICATIONS AND RELATED MATTERS
SEC. 106. FEDERAL PENALTIES FOR THE INTER-
CEPTION OF COMMUNICATIONS.
(a) DEFINITIONS.—Section 2510(1) of title
18, United States Code, is amended—
(C) by striking out “any communication” and
inserting “any aural transfer” in lieu
thereof;
(D) by inserting “(including the use of
such connection in a switching station)” after
“reception”;
(E) by striking out “as a common carrier”;
and
(F) by inserting before the semicolon at the
end of the following: “or communications
affecting interstate or foreign commerce,
but such term does not include the radio
portion of a cordless telephone communica-
tion that is transmitted between the cord-
less 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 elec-
tronic communications”.
(3) Section 2510(4)(1) 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(6)(b) of title 18, United
States Code, is amended by striking out
“identity of the parties to such communica-
tion or the existence,”.
(5) Section 2510 of title 18, United
States Code, is amended—
(A) by striking out “and” at the end of
paragraph (10); and
(B) by striking out the period at the end
of paragraph (11) and inserting a semicolon
thereof.
(12) ‘electronic communication’ means
any transfer of signs, signals, writing,
data, sounds, images, or intelligence of
any nature transmitted in whole or in part by
wire, radio, electromagnetic, photoelectronic
or phonographic means, and also those
effects on interstate or foreign commerce, but
does not include—
(A) the radio portion of a cordless tele-
phone communication that is transmitted
between the cordless telephone handset and
the base unit;
(B) any wire or oral communication;
SEC. 102. REQUIREMENTS FOR CERTAIN DISCLOSURES.

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

"(3)(A) Except as provided in subparagraph (B) of this paragraph, a person or entity providing an electronic communication service to the public upon which willfully 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 original addressee or intended recipient of such communication;

"(iii) to a person employed or authorized, or whose facilities are used, by such a provider of wire or electronic communication service to the public in the course of providing that service; and

"(iv) (B) A person or entity providing wire or 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 original addressee or intended recipient of such communication;

"(iii) to a person employed or authorized, or whose facilities are used, by such a provider of wire or electronic communication service to the public in the course of providing that service; and

"(iv) (C) A customer whose wire, oral, or electronic communication is intercepted, disclosed, or willfully 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 in connection therewith.

(c) COMPUTATION OF DAMAGES.—The court may assess damages in an action under this section in the amount of—

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

"(2) statutory damages of whichever is the greater of $100 or $1,000 for each day of violation;

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

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

"(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 defense to a civil action under this section.

(d) 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. 103. CERTAIN APPROVALS BY JUSTICE DEPARTMENT OFFICIALS.

Section 2516(1) of title 18 of the United States Code is amended by striking out "or" and inserting "and" after "any Assistant Attorney General" and inserting in lieu thereof "any Assistant Attorney General or".
General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General of the Criminal Division; SEC. 105. ADDITION OF OFFENSES TO CRIMES FOR WHICH INTERCEPTION IS AUTHORIZE

(a) WIRE AND ORAL INTERCEPTIONS.—Sec

(b) INTERCEPTION OF ELECTRONIC COMMUNI

(c) COMMENCEMENT OF 30-DAY PERIOD AND POSTPONEMENT OR MINIMIZATION.—Sec

(d) ALTERNATIVE TO DESIGNATING SPECIFIC FACILITIES FROM WHICH COMMUNICATIONS MAY BE INTERCEPTED.—Sec

(e) INTERCEPTION DEVICES.—Sec

(f) DESTRUCTION OF RECORDS.—Sec

(g) STATE AND FOREIGN TRAVEL OR TRANSPORTATION IN SUCH TERM IS DEFINED FOR THE PURPOSES OF THE

(h) INTELLIGENCE ACTIVITIES.—Sec

(i) COMMERCIAL FACILITIES.—Sec

(j) REIMBURSEMENT FOR ASSISTANCE.—Sec

(k) CARE AND PROTECTION OF INTERCEPTORS.—Sec

(l) NOTICE OF CERTAIN ACTIVITIES UNDER PROCEDURES AUTHORIZED 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.

(m) MOBILE TRACKING DEVICES.—In General.—Chapter 205 of title 18, United States Code, is amended by adding at the end the following:

(n) 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:”.

SEC. 2159(1) 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(1)(i)(I) of this title” after “applied for”. SEC. 106. 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 AUTHORIZED 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. 105. ADDITION OF OFFENSES TO CRIMES FOR WHICH INTERCEPTION IS AUTHORIZED;

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

SEC. 107. INTELLIGENCE ACTIVITIES.

Section 1217. 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) EXCEPTIONS.—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 by use of position data derived from a satellite-based global positioning system or similar system.

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:

(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:

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:”.

Whoever, having knowledge that a Federal investigative or law enforcement officer has been authorized or has applied for authority within the territorial jurisdiction of the court in which the judge is sitting;

(12) Any application 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 (i) may be accomplished by the person committing the offense and whose communications are to be intercepted; and

(13) The judge finds that such purpose has been adequately shown.

(12) Application 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 (i) may be accomplished by the person committing the offense and whose communications are to be intercepted; and

(13) The judge finds that such purpose has been adequately shown.

Whoever, having knowledge that a Federal investigative or law enforcement officer has been authorized or has applied for authority within the territorial jurisdiction of the court in which the judge is sitting;
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 for not more than five years, or both.

§211. INJUNCTIVE REMEDY.

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a violation of the provisions 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 or information is filed against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

§2521. Injunction against illegal interception

(a) CONTENTS OF ELECTRONIC COMMUNICATIONS SERVICE.—Section 2511(2)(a) of title 18, United States Code, is amended by adding the following after subsection (a):

"(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, and

(c) EXCEPTIONS.—Subsection (a) of this section does not apply to the rendering of the service or to the protection of the rights or property of the provider of that service or the phone toll and transactional services.

§2701. Unlawful access to stored communications

(a) Offense.—Except as provided in subsection (c) of this section whenever—

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

(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 not authorized or maintained by the user; and

(b) Exemptions.—Subsection (a) of this section does not apply to any such communications for purposes of providing any services other than storage or computer processing.

§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 contents of a communication while in electronic storage by that service;

(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 not authorized or maintained by the user; and

(b) Exemptions.—Subsection (a) of this section does not apply to any such communications for purposes of providing any services other than storage or computer processing.

§2703. Requirements for governmental access

(a) CONTENTS OF ELECTRONIC COMMUNICATIONS SERVICE.—Section 2511(2)(a) of title 18, United States Code, as amended by section 2516, 2511(2)(a), or 2703 of this title:

(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 communications to its destination;

(5) as may be necessary incident to the rendition of the service or to the protection of the rights or property of the provider of that service or the phone toll and transactional services.

§2101. Definitions.

§2701. Unlawful access to stored communications

(a) Offense.—Except as provided in subsection (c) of this section whenever—

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

(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 not authorized or maintained by the user; and

(b) Exemptions.—Subsection (a) of this section does not apply to any such communications for purposes of providing any services other than storage or computer processing.

§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 contents of a communication while in electronic storage by that service;

(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 not authorized or maintained by the user; and

(b) Exemptions.—Subsection (a) of this section does not apply to any such communications for purposes of providing any services other than storage or computer processing.

§2703. Requirements for governmental access

(a) CONTENTS OF ELECTRONIC COMMUNICATIONS SERVICE.—Section 2511(2)(a) of title 18, United States Code, as amended by section 2516, 2511(2)(a), or 2703 of this title:

(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 communications to its destination;

(5) as may be necessary incident to the rendition of the service or to the protection of the rights or property of the provider of that service or the phone toll and transactional services.
"(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (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 showing shall not issue if prohibited by the law of such State.

§ 2704. Backup preservation

"(a) BACKUP PRESERVATION.—(1) A governmental entity acting under section 2703 of this title shall create within two business days after receipt of such request 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 14 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 latter of—

"(A) the delivery of the information; or

"(B) the resolution of any proceedings (including any appeal) concerning the governmental entity's subpoena or court order.

"(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than 14 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) of this section if the government demonstrates to a reasonable standard of proof that such a backup copy is necessary and which have been directly in relation to the investigation or unduly delaying a trial.

"§ 2705. Delayed notice

"(a) DELAY OR NOTIFICATION.—(1) A governmental entity may seek to delay notification under section 2703(b) of this title if the existence of the subpoena or court order may result in—

"(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.

"(2) The governmental entity shall maintain a true copy of certification under paragraph (1) or (4) of this subsection.

"(3) Upon expiration of the period of delay, notification pursuant to paragraph (1) or (4) of this subsection, the governmental entity shall serve, or deliver by registered or first class mail to, the subscriber or customer 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 court which issued such order; and

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

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

"(D) provision of this chapter allowed such delay.

"(b) EXCLUSION 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), (b)(4), or (b)(5), may do so only 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 to—

"(1) in such proceeding, not to notify any other person of the existence of the warrant, subpoena, or court order; and

"(2) in such proceeding, not to notify any other person of the existence of the warrants, subpoenas, or court order, and to—

"(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, pursuant to section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or processing 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 in-
clude any costs due to necessary disruption of normal operations of any electronic communication service or removal of service in which such information may be stored.

(b) AMOUNT.—The amount of the fee provided under subsection (a) shall be mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be determined by the court which issued the order for production of such information (or the court before which a criminal prosecution involving such information may 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 that the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

§ 2707. Civil action.

(a) CAUSE OF ACTION.—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) damages and other equitable or declaratory relief as may be appropriate; and

(2) damages under subsection (c); and

(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 event shall a person entitled to recover receive more than $1,000 and reasonable attorney's fees and other litigation costs reasonably incurred.

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

(1) a court warrant or order, a grand jury equivalent affirmation, or an equivalently valid administrative order or an extension of an order under section 3123 of this title or

(2) a certification by the applicant that

(a) the information sought is relevant to an ongoing criminal investigation; or

(b) the term 'remote computing service' means the provision to the public of computer storage facilities by means of an electronic communications system.

(b) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES CONVENE.—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.

§ 7116. Definitions for chapter.

As used in this chapter—

(1) the terms defined in section 2101 of this title shall have the definitions given such terms in that section; and

(2) the term 'remote computing service' means the provision to the public of computer storage facilities 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.
shall furnish such investigative or law enforcement, or to any other person, unless shall be reasonably compensated for such reasonable expenses incurred in providing a report to Congress on the number of pen register agencies of the Department of Justice.

The term ‘pen register’ means—
(1) the identity, if known, of the person who is the subject of the criminal investigation;
(2) the number and, if known, physical location of the telephone line to which the pen register is to be attached; and
(3) the term ‘court of competent jurisdiction’ means—
(A) a district court of the United States
(B) a court of general jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register;
(C) an attorney for the government or an officer of the United States of any of the United States;
(D) any other person who furnishes facilities or technical assistance pursuant to this section directed by a court order as provided in this section; or
(E) a declarative judgment that—
(1) the target of the wiretap is changing; and
(2) the meaning set forth for such term in section 3121 of this title, has been ordered by the court.

The term ‘wire communication’ has the meaning set forth for such term in section 3121 of this title.

The term ‘communications common carrier’ has the meaning set forth for such term in section 3121 of this title.

The term ‘common carrier’ has the meaning set forth for such term in section 15(h) of this title.

The term ‘carrier communications’ includes video and data communications. The bill expands coverage to include wire communications which a voice wiretap order may be issued. The bill expands the list of felonies for which a 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 particular telephone. The bill announces that the Justice Department makes a showing that the target of the wiretap is changing telephones to thwart interception of his or her communications. The bill makes it a crime for any person who knows of a wiretap to alter any person who willfully accesses without authorization a computer through which an electronic communications system is configured so that such access will result in the interception of communications contained in their systems except under circumstances specified in the bill.

The bill establishes criminal penalties for any person who willfully accesses without authorization a computer through which an electronic communications system is configured so that such access will result in the interception of communications contained in their systems except under circumstances specified in the bill.
The content of messages contained in 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 service without notice to the subscriber pursuant to an administrative subpoena or with notice to the subscriber if the government obtains a warrant under the Federal Rules of Criminal Procedure or equivalent state warrant.

The contents of certain records stored by providers of remote computing 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.

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

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

Mr. MATHIAS. Mr. President, today I am pleased to join with the junior Senator from Vermont, Mr. LEAHY, to introduce the Electronic Communications Privacy Act of 1986. This legislation is an essential element in our efforts to strengthen the protection of Americans' right to privacy in an era of ever more pervasive electronic communications media.

This bill is to introduce today is a revised version of S. 1667, which Senator LEAHY and I introduced on September 19, 1985. It is also identical to H.R. 4562, as unanimously approved earlier this month by the Judiciary Committee of the House of Representatives.

This bill has the same goal as S. 1667: To protect the privacy of Americans against unwanted and unwarranted intrusions. It adopts the same methods to achieve that result as did S. 1667. It incorporates the Federal wiretapping statute to bring fully within its ambit new communications technologies—including electronic mail, cellular telephone, and data transmission between computers—that have transformed the ways in which Americans share information with each other and with the world.

But our earlier bill has been improved by the process of hearings in both the Senate and the House, and extensive negotiations among interested parties in Government, private industry, and civil libertarian. The result is a bill that embodies the theme of wiretapping—promote the development and proliferation of new communications technologies, and respond to the legitimate needs of law enforcement.

Technological advances are fast obliterating the distinction between common carrier and private communications systems. And the means by which information are blurring the line between data in transmission and information in temporary electronic storage.

The legislation responds to these developments by protecting the privacy of information in any electronic form, while it is in transmission or temporary storage, and without regard to the medium of its transmission.

While the bill makes a few distinctions between the treatment of conventional telephone conversations and communications by other media, these differences appear reasonable and do not seriously detract from the principle of adapting American law to the technology of the present and future, rather than the past.

The Electronic Communications Privacy Act of 1986 specifies the circumstances under which law enforcement agencies may seek to intercept electronic communications or intrude into incidental electronic communications storage facilities. It also outlaws those intrusions that are not pursuant to a warrant, and prohibits computer hacking directed against electronic communications systems if the result is to obtain, alter, or prevent access to a communication in the computer. The bill provides standards for third-party access to other data held by the operators of electronic communications services, and gives the customer the same relief that would be available under a court order in civil law enforcement.

Mr. President, the principles underlying this bill have long been supported by the privacy advocates and by the affected communications industries. The benefits of these advances, which have occurred so rapidly and have continued innovation depend upon customer confidence that unauthorized snooping will be deterred and punished. That support continues, and has been strengthened by the improvements made in the bill in the legislative process in the other body. The administration in general, and the Attorney General in particular, have also been on record for a long time in support of the need to bring the wiretap laws up to date with modern technology.

Mr. President, the bill we introduce today adds S. 1667 the useful improvements crafted by our colleagues in the House of Representatives, particularly Representative Robert Kastenmeier, chairman of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, and Representative Carlos Moorhead, that subcommittee's ranking minority member. I urge Senators to examine this legislation, to understand and provide for it. It would be necessary, and to join with me and with Senator LEAHY to see that it is speedily enacted into law.

By Mr. DURENBERGER (for himself, Mr. BAUCUS, Mr. DOLE, Mr. CHAFFEE, Mr. HEINZ, Mr. CHILES, Mr. ANDERSON, and Mr. MITCHELL):

S. 2576. A bill to amend title XVIII of the Social Security Act to require timely payment of properly submitted Medicare claims; to the Committee on Finance.

Mr. DURENBERGER. Mr. President, the principles underlying this bill have long been supported by privacy advocates and by the affected communications industries. The benefits of these advances, which have occurred so rapidly and have continued innovation depend upon customer confidence that unauthorized snooping will be deterred and punished. That support continues, and has been strengthened by the improvements made in the bill in the legislative process in the other body. The administration in general, and the Attorney General in particular, have also been on record for a long time in support of the need to bring the wiretap laws up to date with modern technology.

Mr. President, the bill we introduce today adds S. 1667 the useful improvements crafted by our colleagues in the House of Representatives, particularly Representative Robert Kastenmeier, chairman of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, and Representative Carlos Moorhead, that subcommittee's ranking minority member. I urge Senators to examine this legislation, to understand and provide for it. It would be necessary, and to join with me and with Senator LEAHY to see that it is speedily enacted into law.

Mr. President, the bill we introduce today adds S. 1667 the useful improvements crafted by our colleagues in the House of Representatives, particularly Representative Robert Kastenmeier, chairman of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, and Representative Carlos Moorhead, that subcommittee's ranking minority member. I urge Senators to examine this legislation, to understand and provide for it. It would be necessary, and to join with me and with Senator LEAHY to see that it is speedily enacted into law.

Mr. President, the bill we introduce today adds S. 1667 the useful improvements crafted by our colleagues in the House of Representatives, particularly Representative Robert Kastenmeier, chairman of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, and Representative Carlos Moorhead, that subcommittee's ranking minority member. I urge Senators to examine this legislation, to understand and provide for it. It would be necessary, and to join with me and with Senator LEAHY to see that it is speedily enacted into law.

Mr. President, the bill we introduce today adds S. 1667 the useful improvements crafted by our colleagues in the House of Representatives, particularly Representative Robert Kastenmeier, chairman of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, and Representative Carlos Moorhead, that subcommittee's ranking minority member. I urge Senators to examine this legislation, to understand and provide for it. It would be necessary, and to join with me and with Senator LEAHY to see that it is speedily enacted into law.

Mr. President, the bill we introduce today adds S. 1667 the useful improvements crafted by our colleagues in the House of Representatives, particularly Representative Robert Kastenmeier, chairman of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, and Representative Carlos Moorhead, that subcommittee's ranking minority member. I urge Senators to examine this legislation, to understand and provide for it. It would be necessary, and to join with me and with Senator LEAHY to see that it is speedily enacted into law.

Mr. President, the bill we introduce today adds S. 1667 the useful improvements crafted by our colleagues in the House of Representatives, particularly Representative Robert Kastenmeier, chairman of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, and Representative Carlos Moorhead, that subcommittee's ranking minority member. I urge Senators to examine this legislation, to understand and provide for it. It would be necessary, and to join with me and with Senator LEAHY to see that it is speedily enacted into law.

Mr. President, the bill we introduce today adds S. 1667 the useful improvements crafted by our colleagues in the House of Representatives, particularly Representative Robert Kastenmeier, chairman of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, and Representative Carlos Moorhead, that subcommittee's ranking minority member. I urge Senators to examine this legislation, to understand and provide for it. It would be necessary, and to join with me and with Senator LEAHY to see that it is speedily enacted into law.

Mr. President, the bill we introduce today adds S. 1667 the useful improvements crafted by our colleagues in the House of Representatives, particularly Representative Robert Kastenmeier, chairman of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, and Representative Carlos Moorhead, that subcommittee's ranking minority member. I urge Senators to examine this legislation, to understand and provide for it. It would be necessary, and to join with me and with Senator LEAHY to see that it is speedily enacted into law.

Mr. President, the bill we introduce today adds S. 1667 the useful improvements crafted by our colleagues in the House of Representatives, particularly Representative Robert Kastenmeier, chairman of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, and Representative Carlos Moorhead, that subcommittee's ranking minority member. I urge Senators to examine this legislation, to understand and provide for it. It would be necessary, and to join with me and with Senator LEAHY to see that it is speedily enacted into law.

Mr. President, the bill we introduce today adds S. 1667 the useful improvements crafted by our colleagues in the House of Representatives, particularly Representative Robert Kastenmeier, chairman of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, and Representative Carlos Moorhead, that subcommittee's ranking minority member. I urge Senators to examine this legislation, to understand and provide for it. It would be necessary, and to join with me and with Senator LEAHY to see that it is speedily enacted into law.

Mr. President, the bill we introduce today adds S. 1667 the useful improvements crafted by our colleagues in the House of Representatives, particularly Representative Robert Kastenmeier, chairman of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, and Representative Carlos Moorhead, that subcommittee's ranking minority member. I urge Senators to examine this legislation, to understand and provide for it. It would be necessary, and to join with me and with Senator LEAHY to see that it is speedily enacted into law.