

Congress, and look forward to working with my colleagues to accomplish this goal.

While on the subject of the Coast Guard authorization bill, I would also like to mention that we Alaskans are pleased with the new Commandant, Adm. Robert Kramek, who took over for Admiral Kime on June 1, 1994.

Admiral Kramek served as Chief of Naval Engineering for the 17th District in Juneau, receiving a masters degree from the University of Alaska, and later served as Commanding Officer aboard a high endurance cutter on enforcement missions in the North Pacific and Bering Sea.

We look forward to working with Admiral Kramek, and are glad that he brings Alaska experience to his new job.

Thank you.

By Mr. LEAHY:

S. 2375. A bill to amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other purposes; to the Committee on Commerce, Science, and Transportation.

THE DIGITAL TELEPHONE ACT OF 1994

Mr. LEAHY. Mr. President, there was a time when law enforcement, if they wanted to listen in to what criminals were saying, the local sheriff could drive down the road, climb on the top of his car, plug a couple alligator clips on to a telephone wire, put on the earphones and know what was being said.

A lot has changed since that time. One of the things that changed, of course, is that we passed legislation laying out who could eavesdrop, when they could listen in and who could be eavesdropped on. We made it very clear: You had to apply to a court and get a warrant. We set good standards to protect your privacy, my privacy, the privacy of everybody in this country. So the standards are there, but the alligator clips have changed.

Now, with digital transmissions, if you were to go down and listen in on a phone line, you probably would just hear a loud buzz. A drug dealer in Boston, MA, who wants to talk with a supplier in Dade County, FL, may pick up a cellular phone that may send out a digital signal, which is nothing more than ones and zeros. This conversation may go through a half-dozen different linkages. It may go any way but a straight line from Boston to Florida, and a lot of it could be over fiber optic cables. And even if you could find the right cable, even if you could find the one conversation out of several thousand conversations carried over the same cable that was the one the court order allowed you to tap, you might hear nothing but a buzz. That is not going to help much to catch that drug spin or to stop that kidnapping or stop a planned assassination or stop any other serious felony.

Because of this loss of ability to keep up with technology, Louis Freeh, the FBI Director, said, "The number one law enforcement, public safety, and national security issue facing us today" is preserving the ability to conduct wiretaps.

So what I am doing is introducing a bill that will give our law enforcement agencies back the confidence that when they get a wiretap order, they will be able to do their jobs and carry out the order. This will allow wiretaps under court orders to be able to be used even with the new digital technology and other emerging telecommunications technologies. This bill will not impede new technologies but ensure they will not confound legitimate law enforcement needs.

Now when this was first proposed—first in the last administration and early on in this administration—I opposed the idea, because it appeared to me that not only were there inadequate safeguards to protect the individual privacy of all of us, but I was very concerned that it was going to set up the Justice Department as some kind of a traffic cop on new technologies.

One of the things that allows us to compete with the rest of the world, especially in our ability to export, is the genius of our technology and our ability to fashion new technology. I was concerned that we would no longer be able to do so and that the Justice Department could say, "Hold it, we don't want you to put in speed dial, we don't want you to put in call forwarding or anything else because it doesn't fit what we want."

This worried me, because, unfortunately, the Federal Government has adamantly and steadfastly stayed 10 to 15 years behind most emerging technologies. We have seen it here in the Senate, where we have had to use antiquated computer systems. We have seen it at the Department of Defense, where they have communications systems that look like they are something out of World War II and not out of the Star Wars they talk about.

Private industry has gone way ahead of the Federal Government in technology and computers and telecommunications, and I did not want it held back.

So what we have done now is put together a bill—Congressman EDWARDS, in the House, and myself—that will help law enforcement. But it also contains important expansions of privacy protection for transactional information, mobile phone communications, certain radio-based communications, and will not impede technology.

Regarding the issue of digital telephony, it should be noted we came an enormous way after countless meetings and literally hundreds of hours of work by people in the private sector, law enforcement, FBI Director Freeh, Members of the House and Senate and staff. But throughout all of this, the person who worked tirelessly and was involved

in every single part of it was, and is, attorney Beryl Howell of the Judiciary Committee staff assigned to my Subcommittee on Technology and the Law.

Beryl Howell is a former prosecutor from the U.S. attorneys office in New York. She is a tremendous litigator, brilliant lawyer, and I think it is safe to say that without her work and her dedication, we would not be introducing this bill today.

Now that the crime conference is concluded, we expect to be considering the conference report shortly. The crime bill does not confront what Louis Freeh, the FBI Director, has identified as "the number one law enforcement, public safety, and national security issue facing us today."

That issue is wiretaps, and law enforcement's losing battle to keep up with new technologies that undermine its capability to use this powerful tool in its crime-fighting arsenal.

There is no doubt that wiretaps can produce powerful evidence against our most dangerous criminals. Instead of making deals with other criminals, or putting innocent bystanders at risk in order to have witnesses who can testify about a defendant's crimes, the police use wiretaps to catch and convict criminals with secretly taped words from their own mouths.

But the FBI and other law enforcement agencies have told Congress that their ability to use this tool is being undercut by new communications features and services that were designed with no thought as to how they might affect law enforcement.

Over the past few months, I have worked closely with Representative DON EDWARDS, chairman of the House Judiciary Subcommittee on Civil and Constitutional Rights, to write the bill I introduce today that addresses the No. 1 problem facing law enforcement today. Industry groups, privacy and civil liberties experts, and the FBI have worked diligently with us in this effort, and I applaud them for undertaking this difficult task. I look forward to hearing from these groups at a joint hearing with DON EDWARDS' Subcommittee this Thursday, with a view to making this bill even better.

My goal in this legislation is to assist legitimate law enforcement needs without jeopardizing privacy rights or frustrating the development of new communications technologies or the competitiveness of America's high-technology industry. I believe this bill achieves that goal.

This is not the first time that Congress has had to take a close look at the wiretap statute to take into account developments in communications technology and the structure of the telecommunications industry. We last did so in 1986 when we passed the Electronic Communications Privacy Act.

This law extended the reach of the Federal wiretap law, and its privacy protections, to electronic mail and

computer-to-computer communications.

In February, FBI Director Freeh came to me and other Members of Congress to consult about a proposal to revise our wiretap law anew in the face of the increasing pace of advances in telecommunications technology and impediments to execution of court-ordered wiretaps. The Clinton administration followed up last March by sending Congress proposed legislation that made significant improvements to an earlier Bush administration draft proposal. We have built on those improvements to address the significant concerns that remained.

First, to ensure law enforcement's continued ability to conduct court-authorized wiretaps in light of new and emerging digital technologies, the bill sets forth four wiretap capability requirements that telecommunications carriers would be required to meet. This means that when the phone companies set about designing and deploying new services or features, they must consider law enforcement's needs among the numerous other factors that go into such designs.

Just as phone companies make sure that when they plug-in new services, the phone system is not shorted-out, so too we do not want to shortchange the American people's need for effective law enforcement.

Second, on the privacy front, the bill expands privacy and security protections for our telephone and computer communications in ways that were first recommended to me by a privacy and technology task force I organized in 1991. The protections of the Electronic Communications Privacy Act are extended to cordless phones and certain data communications transmitted by radio.

In addition, this bill increases the protection for transactional data on electronic communications services by requiring law enforcement to get a court order for access to those records.

The bill further protects privacy by requiring telecommunications systems to protect communications not authorized to be intercepted and by restricting the ability of law enforcement to use pen register devices for tracking purposes or for obtaining transactional information. Finally, the bill improves the privacy of mobile phones by expanding criminal penalties for stealing the service from legitimate users.

Third, to encourage innovation in telecommunications services, the bill states expressly that law enforcement agencies may not require the specific design of telecommunications systems or features, nor prohibit adoption of any such design, by any telecommunications provider.

The bill sets up a mechanism for ensuring law enforcement's wiretap capability needs while at the same time deferring to industry to decide how best to meet law enforcement's wiretap needs. No Government official will be

put in charge of the future of our telecommunications industry.

This legislation leaves it to industry in the first instance.

But I also do not want industry and law enforcement representatives to get together in some back room and figure out how to wiretap America. It is important that this process be subject to public scrutiny, oversight, and accountability. This bill accomplishes this by requiring any standards or technical requirements that industry adopts to ensure wiretap capability be publicly available.

Furthermore, this bill avoids putting industry in the position of guaranteeing wiretap capability, with failure punished by stopping a service or feature that consumers want. If industry is ready to deploy a new phone feature or service, but cannot yet figure out how to give law enforcement access for lawful wiretaps, a court must take that into consideration and may not stop deployment of the service. On the other hand, if industry can fix the service to assist law enforcement, it must do so.

This bill preserves a legitimate law enforcement tool without jeopardizing privacy rights or frustrating innovation and the development of new technologies or undercutting the competitiveness of America's high-technology industries.

Mr. President, I ask unanimous consent that the legislation and a section-by-section analysis be inserted in the RECORD.

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

S. 2375

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

SECTION 1. INTERCEPTION OF DIGITAL AND OTHER COMMUNICATIONS.

(a) IN GENERAL.—Part I of title 18, United States Code, is amended by inserting after chapter 119 the following new chapter:

CHAPTER 120—TELECOMMUNICATIONS CARRIER ASSISTANCE TO THE GOVERNMENT

“Sec.

“2601. Definitions.

“2602. Assistance capability requirements.

“2603. Notices of capacity requirements.

“2604. Systems security and integrity.

“2605. Cooperation of equipment manufacturers and providers of telecommunications support services.

“2606. Technical requirements and standards; extension of compliance date.

“2607. Enforcement orders.

“2608. Reimbursement of telecommunications carriers.

“§ 2601. Definitions

“(a) DEFINITIONS.—In this chapter—

“the terms defined in section 2510 have, respectively, the meanings stated in that section.

“‘call-identifying information’—

“(A) means all dialing or signalling information associated with the origin, direction, destination, or termination of each communication generated or received by the subscriber equipment, facility, or service of a telecommunications carrier that is the sub-

ject of a court order or lawful authorization; but

“(B) does not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number).

“‘Commission’ means the Federal Communications Commission.

“‘government’ means the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any State or political subdivision thereof authorized by law to conduct electronic surveillance.

“‘information services’—

“(A) means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and

“(B) includes electronic publishing and messaging services; but

“(C) does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.

“‘provider of telecommunications support services’ means a person or entity that provides a product, software, or service to a telecommunications carrier that is integral to such carrier's switching or transmission of wire or electronic communications.

“‘telecommunications carrier’—

“(A) means a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire (within the meaning of section 3(h) of the Communications Act of 1934 (47 U.S.C. 153(h))); and

“(B) includes—

“(i) a person or entity engaged in providing commercial mobile service (as defined in section 332(d) of the Communications Act of 1934 (47 U.S.C. 332(d))); and

“(ii) a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this chapter; but

“(C) does not include persons or entities insofar as they are engaged in providing information services.

“§ 2602. Assistance capability requirements

“(a) CAPABILITY REQUIREMENTS.—Except as provided in subsections (b), (c), and (d) of this section, and subject to section 2607(c), a telecommunications carrier shall ensure that its services or facilities that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of—

“(1) expeditiously isolating and enabling the government to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's service, facility, or equipment or at such later time as may be acceptable to the government;

“(2) expeditiously isolating and enabling the government to access call-identifying information that is reasonably available to the carrier—

“(A) before, during, or immediately after the transmission of a wire or electronic com-

munication (or at such later time as may be acceptable to the government); and

"(B) in a manner that allows it to be associated with the communication to which it pertains.

except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number);

"(3) delivering intercepted communications and call-identifying information to the government in a format such that they may be transmitted by means of facilities or services procured by the government to a location other than the premises of the carrier; and

"(4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects—

"(A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and

"(B) information regarding the government's interception of communications and access to call-identifying information.

"(b) LIMITATIONS.—

"(1) DESIGN OF FEATURES AND SYSTEMS CONFIGURATIONS.—This chapter does not authorize any law enforcement agency or officer—

"(A) to require any specific design of features or system configurations to be adopted by providers of wire or electronic communication service, manufacturers of telecommunications equipment, or providers of telecommunications support services; or

"(B) to prohibit the adoption of any feature or service by providers of wire or electronic communication service, manufacturers of telecommunications equipment, or providers of telecommunications support services.

"(2) INFORMATION SERVICES AND INTERCONNECTION SERVICES AND FACILITIES.—The requirements of subsection (a) do not apply to—

"(A) information services; or

"(B) services or facilities that support the transport or switching of communications for the sole purpose of interconnecting telecommunications carriers or private networks.

"(3) ENCRYPTION.—A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.

"(c) EMERGENCY OR EXIGENT CIRCUMSTANCES.—In emergency or exigent circumstances (including those described in sections 2518 (7) or (11)(b) and 3125 of this title and section 1805(e) of title 50), a carrier may fulfill its responsibilities under subsection (a)(3) by allowing monitoring at its premises if that is the only means of accomplishing the interception or access.

"(d) MOBILE SERVICE ASSISTANCE REQUIREMENTS.—A telecommunications carrier offering a feature or service that allows subscribers to redirect, hand off, or assign their wire or electronic communications to another service area or another service provider or to utilize facilities in another service area or another service provider shall ensure that, when the carrier that had been providing assistance for the interception of wire or elec-

tronic communications or access to call-identifying information pursuant to a court order or lawful authorization no longer has access to the content of such communications or call-identifying information within the service area in which interception has been occurring as a result of the subscriber's use of such a feature or service, information is available to the government (before, during, or immediately after the transfer of such communications) identifying the provider of wire or electronic communication service that has acquired access to the communications.

"§ 2603. Notices of capacity requirements

"(a) NOTICES OF MAXIMUM AND INITIAL CAPACITY REQUIREMENTS.—

"(1) IN GENERAL.—Not later than 1 year after the date of enactment of this chapter, and after consulting with State and local law enforcement agencies, telecommunications carriers, providers of telecommunications support services, and manufacturers of telecommunications equipment, the Attorney General shall publish in the Federal Register and provide to appropriate telecommunications carrier associations, standard-setting organizations, and for a—

"(A) notice of the maximum capacity required to accommodate all of the communication interceptions, pen registers, and trap and trace devices that the Attorney General estimates that government agencies authorized to conduct electronic surveillance may conduct and use simultaneously; and

"(B) notice of the number of communication interceptions, pen registers, and trap and trace devices, representing a portion of the maximum capacity set forth under subparagraph (A), that the Attorney General estimates that government agencies authorized to conduct electronic surveillance may conduct and use simultaneously after the date that is 4 years after the date of enactment of this chapter.

"(2) BASIS OF NOTICES.—The notices issued under paragraph (1) may be based upon the type of equipment, type of service, number of subscribers, geographic location, or other measure.

"(b) COMPLIANCE WITH CAPACITY NOTICES.—

"(1) INITIAL CAPACITY.—Within 3 years after the publication by the Attorney General of a notice of capacity requirements or within 4 years after the date of enactment of this chapter, whichever is longer, a telecommunications carrier shall ensure that its systems are capable of—

"(A) expanding to the maximum capacity set forth in the notice under paragraph (1)(A); and

"(B) accommodating simultaneously the number of interceptions, pen registers, and trap and trace devices set forth in the notice under paragraph (1)(B).

"(2) PERMANENT CAPACITY.—After the date described in paragraph (1), a telecommunications carrier shall ensure that it can accommodate expeditiously any increase in the number of communication interceptions, pen registers, and trap and trace devices that authorized agencies may seek to conduct and use, up to the maximum capacity requirement set forth in the notice under paragraph (1)(A).

"(c) NOTICES OF INCREASED MAXIMUM CAPACITY REQUIREMENTS.—

"(1) The Attorney General shall periodically provide to telecommunications carriers written notice of any necessary increases in the maximum capacity requirement set forth in the notice under subsection (b)(1).

"(2) Within 3 years after receiving written notice of increased capacity requirements under paragraph (1), or within such longer time period as the Attorney General may

specify, a telecommunications carrier shall ensure that its systems are capable of expanding to the increased maximum capacity set forth in the notice.

"§ 2604. Systems security and integrity

"A telecommunications carrier shall ensure that any court ordered or lawfully authorized interception of communications or access to call-identifying information effected within its switching premises can be activated only with the affirmative intervention of an individual officer or employee of the carrier.

"§ 2605. Cooperation of equipment manufacturers and providers of telecommunications support services

"(a) CONSULTATION.—A telecommunications carrier shall consult, as necessary, in a timely fashion with manufacturers of its telecommunications transmission and switching equipment and its providers of telecommunications support services for the purpose of identifying any service or equipment, including hardware and software, that may require modification so as to permit compliance with this chapter.

"(b) MODIFICATION OF EQUIPMENT AND SERVICES.—Subject to section 2607(c), a manufacturer of telecommunications transmission or switching equipment and a provider of telecommunications support services shall, on a reasonably timely basis and at a reasonable charge, make available to the telecommunications carriers using its equipment or services such modifications as are necessary to permit such carriers to comply with this chapter.

"§ 2606. Technical requirements and standards; extension of compliance date

"(a) SAFE HARBOR.—

"(1) CONSULTATION.—To ensure the efficient and industry-wide implementation of the assistance capability requirements under section 2602, the Attorney General, in coordination with other Federal, State, and local law enforcement agencies, shall consult with appropriate associations and standard-setting organizations of the telecommunications industry.

"(2) COMPLIANCE UNDER ACCEPTED STANDARDS.—A telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 2602, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found to be in compliance with section 2605, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards are adopted by an industry association or standard-setting organization or by the Commission under subsection (b) to meet the requirements of section 2602.

"(3) ABSENCE OF STANDARDS.—The absence of technical requirements or standards for implementing the assistance capability requirements of section 2602 shall not—

"(A) preclude a carrier, manufacturer, or services provider from deploying a technology or service; or

"(B) relieve a carrier, manufacturer, or service provider of the obligations imposed by section 2602 or 2605, as applicable.

"(b) FCC AUTHORITY.—

"(1) IN GENERAL.—If industry associations or standard-setting organizations fail to issue technical requirements or standards or if a government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the Commission to establish, by notice and comment rulemaking or such other proceedings as the Commission may be authorized to conduct, technical requirements or standards that—

"(A) meet the assistance capability requirements of section 2602;

"(B) protect the privacy and security of communications not authorized to be intercepted; and

"(C) serve the policy of the United States to encourage the provision of new technologies and services to the public.

"(2) TRANSITION PERIOD.—If an industry technical requirement or standard is set aside or supplanted as a result of Commission action under this section, the Commission, after consultation with the Attorney General, shall establish a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under section 2602 during any transition period.

"(c) EXTENSION OF COMPLIANCE DATE FOR FEATURES AND SERVICES.—

"(1) PETITION.—A telecommunications carrier proposing to deploy, or having deployed, a feature or service within 4 years after the date of enactment of this chapter may petition the Commission for 1 or more extensions of the deadline for complying with the assistance capability requirements under section 2602.

"(2) GROUND FOR EXTENSION.—The Commission may, after affording a full opportunity for hearing and after consultation with the Attorney General, grant an extension under this paragraph, if the Commission determines that compliance with the assistance capability requirements under section 2602 is not reasonably achievable through application of technology available within the compliance period.

"(3) LENGTH OF EXTENSION.—An extension under this paragraph shall extend for no longer than the earlier of—

"(A) the date determined by the Commission as necessary for the carrier to comply with the assistance capability requirements under section 2602; or

"(B) the date that is 2 years after the date on which the extension is granted.

"(4) APPLICABILITY OF EXTENSION.—An extension under this subsection shall apply to only that part of the carrier's business on which the new feature or service is used.

"§ 2607. Enforcement orders

"(a) ENFORCEMENT BY COURT ISSUING SURVEILLANCE ORDER.—If a court authorizing an interception under chapter 119, a State statute, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or authorizing use of a pen register or a trap and trace device under chapter 206 or a State statute finds that a telecommunications carrier has failed to comply with the requirements in this chapter, the court may direct that the carrier comply forthwith and may direct that a provider of support services to the carrier or the manufacturer of the carrier's transmission or switching equipment furnish forthwith modifications necessary for the carrier to comply.

"(b) ENFORCEMENT UPON APPLICATION BY ATTORNEY GENERAL.—The Attorney General may apply to the appropriate United States district court for, and the United States district courts shall have jurisdiction to issue, an order directing that a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services comply with this chapter.

"(c) GROUNDS FOR ISSUANCE.—A court shall issue an order under subsections (a) or (b) only if the court finds that—

"(1) alternative technologies or capabilities or the facilities of another carrier are not reasonably available to law enforcement for implementing the interception of com-

munications or access to call-identifying information; and

"(2) compliance with the requirements of this chapter is reasonably achievable through the application of available technology to the feature or service at issue or would have been reasonably achievable if timely action had been taken.

"(d) TIME FOR COMPLIANCE.—Upon issuance of an enforcement order under this section, the court shall specify a reasonable time and conditions for complying with its order, considering the good faith efforts to comply in a timely manner, any effect on the carrier's, manufacturer's, or service provider's ability to continue to do business, the degree of culpability or delay in undertaking efforts to comply, and such other matters as justice may require.

"(e) LIMITATION.—An order under this section may not require a telecommunications carrier to meet the government's demand for interception of communications and acquisition of call-identifying information to any extent in excess of the capacity for which notice has been provided under section 2603.

"(f) CIVIL PENALTY.—

"(1) IN GENERAL.—A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to \$10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify.

"(2) CONSIDERATIONS.—In determining whether to impose a fine and in determining its amount, the court shall take into account—

"(A) the nature, circumstances, and extent of the violation;

"(B) the violator's ability to pay, the violator's good faith efforts to comply in a timely manner, any effect on the violator's ability to continue to do business, the degree of culpability, and the length of any delay in undertaking efforts to comply; and

"(C) such other matters as justice may require.

"(3) CIVIL ACTION.—The Attorney General may file a civil action in the appropriate United States district court to collect, and the United States district courts shall have jurisdiction to impose, such fines.

"§ 2608. Reimbursement of telecommunications carriers

"(a) IN GENERAL.—The Attorney General shall, subject to the availability of appropriations, reimburse telecommunications carriers for all reasonable costs directly associated with—

"(1) the modifications performed by carriers prior to the effective date of section 2602 or prior to the expiration of any extension granted under section 2605(c) to establish the capabilities necessary to comply with section 2602;

"(2) meeting the maximum capacity requirements set forth in the notice under section 2603(a)(1)(A); and

"(3) expanding existing facilities to accommodate simultaneously the number of interceptions, pen registers and trap and trace devices for which notice has been provided under section 2603(a)(1)(B).

"(b) PROCEDURES AND REGULATIONS.—Notwithstanding any other law, the Attorney General may establish any procedures and regulations deemed necessary to effectuate timely and cost-efficient reimbursement to telecommunications carriers for reimbursable costs incurred under this chapter, under chapters 119 and 121, and under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

"(c) DISPUTE RESOLUTION.—If there is a dispute between the Attorney General and a telecommunications carrier regarding the amount of reasonable costs to be reimbursed under subsection (b), the dispute shall be resolved and the amount determined in a proceeding initiated at the Commission under section 2606(b) or by the court from which an enforcement order is sought under section 2607.

"(d) LACK OF APPROPRIATED FUNDS.—The lack of appropriated funds sufficient to reimburse telecommunications carriers for modifications under subsection (a) shall be considered by the Commission or a court in determining whether compliance is reasonable under section 2607(c).

(b) TECHNICAL AMENDMENT.—The part analysis for part I of title 18, United States Code, is amended by inserting after the item relating to chapter 119 the following new item:

"120. Telecommunications carrier assistance to the Government 2601".

SEC. 2. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to carry out section 2608 of title 18, United States Code, as added by section 1—

(1) a total of \$500,000,000 for fiscal years 1995, 1996, 1997, and 1998; and

(2) such sums as are necessary for each fiscal year thereafter.

SEC. 3. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in paragraph (2), chapter 120 of title 18, United States Code, as added by section 1, shall take effect on the date of enactment of this Act.

(b) ASSISTANCE CAPABILITY AND SYSTEMS SECURITY AND INTEGRITY REQUIREMENTS.—Sections 2602 and 2604 of title 18, United States Code, as added by section 1, shall take effect on the date that is 4 years after the date of enactment of this Act.

SEC. 4. REPORTS.

(a) REPORTS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—On or before November 30, 1995, and on or before November 30 of each year for 5 years thereafter, the Attorney General shall submit to the Congress a report on the amounts paid during the preceding fiscal year in reimbursement to telecommunications carriers under section 2608 of title 18, United States Code, as added by section 1.

(2) CONTENTS.—A report under paragraph (1) shall include—

(A) a detailed accounting of the amounts paid to each carrier and the technology, feature or service for which the amounts were paid; and

(B) projections of the amounts expected to be paid in the current fiscal year, the carriers to which reimbursement is expected to be paid, and the technologies, services, or features for which reimbursement is expected to be paid.

(b) REPORTS BY THE COMPTROLLER GENERAL.—

(1) IN GENERAL.—On or before April 1, 1996, and April 1, 1998, the Comptroller General of the United States, after consultation with the Attorney General and the telecommunications industry, shall submit to the Congress a report reflecting its audit of the sums paid by the Attorney General to carriers in reimbursement.

(2) CONTENTS.—A report under paragraph (1) shall include the findings and conclusions of the Comptroller General on the costs to be incurred after the compliance date, including projections of the amounts expected to be incurred and the technologies, services, or features for which expenses are expected to be incurred.

SEC. 5. CORDLESS TELEPHONES.

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

(1) in paragraph (1) by striking "but such term does not include" and all that follows through "base unit"; and

(2) in paragraph (2) by striking subparagraph (A) and redesignating subparagraphs (B), (C), and (D) as subparagraphs (A), (B), and (C), respectively.

(b) **PENALTY.**—Section 2511 of title 18, United States Code, is amended—

(1) in subsection (4)(b)(i) by inserting "a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit," after "cellular telephone communication,"; and

(2) in subsection (4)(b)(ii) by inserting "a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit," after "cellular telephone communication,".

SEC. 6. RADIO-BASED DATA COMMUNICATIONS.

Section 2510(16) of title 18, United States Code, is amended—

(1) by striking "or" at the end of subparagraph (D);

(2) by inserting "or" at the end of subparagraph (E); and

(3) by inserting after subparagraph (E) the following new subparagraph:

"(F) an electronic communication;"

SEC. 7. PENALTIES FOR MONITORING RADIO COMMUNICATIONS THAT ARE TRANSMITTED USING MODULATION TECHNIQUES WITH NONPUBLIC PARAMETERS.

Section 2511(4)(b) of title 18, United States Code, is amended by striking "or encrypted, then" and inserting "encrypted, or transmitted using modulation techniques the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication".

SEC. 8. TECHNICAL CORRECTION.

Section 2511(2)(a)(1) of title 18, United States Code, is amended by striking "used in the transmission of a wire communication" and inserting "used in the transmission of a wire or electronic communication".

SEC. 9. FRAUDULENT ALTERATION OF COMMERCIAL MOBILE RADIO INSTRUMENTS.

(a) **OFFENSE.**—Section 1029(a) of title 18, United States Code, is amended—

(1) by striking "or" at the end of paragraph (3); and

(2) by inserting after paragraph (4) the following new paragraphs:

"(5) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services; or

"(6) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses—

"(A) a scanning receiver; or

"(B) hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services."

(b) **PENALTY.**—Section 1029(c)(2) of title 18, United States Code, is amended by striking "(a)(1) or (a)(4)" and inserting "(a) (1), (4), (5), or (6)".

(c) **DEFINITIONS.**—Section 1029(e) of title 18, United States Code, is amended—

(1) in paragraph (1) by inserting "electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier," after "account number,";

(2) by striking "and" at the end of paragraph (5);

(3) by striking the period at the end of paragraph (6) and inserting "and"; and

(4) by adding at the end the following new paragraph:

"(7) the term 'scanning receiver' means a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119."

SEC. 10. TRANSACTIONAL DATA.

(a) **DISCLOSURE OF RECORDS.**—Section 2703 of title 18, United States Code, is amended—

(1) in subsection (c)—

(A) in subparagraph (B)—

(i) by striking clause (i); and

(ii) by redesignating clauses (ii), (iii), (iv) as clauses (i), (ii), and (iii), respectively; and

(B) by adding at the end the following new subparagraph:

"(C) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the name, billing address, and length of service of a subscriber to or customer of such service and the types of services the subscriber or customer utilized, when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under subparagraph (B)."; and

(2) by amending the first sentence of subsection (d) to read as follows: "A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction described in section 3126(2)(A) and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."

(b) **PEN REGISTERS AND TRAP AND TRACE DEVICES.**—Section 3121 of title 18, United States Code, is amended—

(1) by redesignating subsection (c) as subsection (d); and

(2) by inserting after subsection (b) the following new subsection:

"(c) **LIMITATION.**—A government agency authorized to install and use a pen register under this chapter or under State law, shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing."

SECTIONAL SUMMARY

The bill consists of the following ten sections:

Sections 1 through 4 deal with law enforcement's wiretap capability and capacity needs.

Sections 5 through 7 expands the privacy protection of the Electronic Communications Privacy Act to cover cordless phones and certain radio-based communications, and Section 8 makes a technical correction to that law.

Section 9 improves the privacy and security of communications over cellular telephones by prohibiting the fraudulent alteration of such telephones for the purpose of stealing service.

Section 10 protects the privacy of electronic communications by requiring a court order for the disclosure of transactional data and by limiting the use of pen registers that intercept information other than dialing or signaling information.

Section 1. Interception of digital and other communications. This section adds a new chapter 120 to title 18, United States Code, to define more precisely the assistance that telecommunications carriers are required to provide in connection with court orders for wire and electronic interceptions, pen registers and trap and trace devices. This new chapter contains eight sections numbered 2601 through 2608.

Section 2601 provides definitions for "call-identifying information," "information services," "government," "providers of telecommunication support services," "telecommunications carrier."

A "Telecommunications carrier" is defined as any person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire, as defined by section 3(h) of the Communications Act of 1934, and includes a commercial mobile service, as defined in section 332(d) of the Communications Act. This definition encompasses such service providers as local exchange carriers, interexchange carriers, competitive access providers (CAPS), cellular carriers, providers of personal communications services (PCS), satellite-based service providers, and any other common carrier who offers wireline or wireless service for hire to the public. It does not include persons or entities to the extent engaged in providing information services, such as electronic mail providers, on-line services providers, such as CompuServe, Prodigy, America On line or Mead Data, or commercial Internet providers. It also does not include "enhanced services" as defined by the FCC at the time of this Act. Such "enhanced services" do not include call forwarding, speed dialing, or the call forwarding portion of a voice mail service.

In addition, for purposes of this Act, the FCC is authorized to deem other persons and entities to be telecommunications carriers subject to the assistance requirements in section 2602 to the extent that such person or entity serves as a replacement for the local telephone service to a substantial portion of the public within a state. Such an entity would satisfy the criteria for a "local exchange carrier" under section 101(b)(j) H.R. 3626, passed by the U.S. House of Representatives on June 28, 1994. As part of its determination whether the public interest is served by deeming a person or entity a telecommunications carrier for the purposes of this Act, the Commission shall consider whether such determination would promote competition, encourage the development of new technologies, and protect public safety and national security.

The term "call-identifying information" means the dialing or signaling information generated which identifies the origin and destination of a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful authorization. For voice communications, this information is typically the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted. In pen register investigations, these pulses, tones, or messages identify the numbers dialed from the facility that is the subject of the court order authorization. In trap and trace investigations, these are the incoming pulses, tones, or messages which identify the originating number of the facility from which the call was placed and which are captured when directed to the facility that is the subject of the court order or authorization.

The term "government" means the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any state or political subdivision thereof authorized by law to conduct electronic surveillance.

The term "provider of telecommunications support services" means any person or entity that provides products, software or services to a common carrier that are integral to the switching of transmissions for wire or electronic communications. There are currently over one hundred such support service

11060

providers that provide common carriers with specialized support services.

Section 2602, entitled "Assistance capability requirements," consists of four subsections. Subsection (a) sets forth four "Capability Requirements," which every telecommunications carrier is required to meet in connection with those services or facilities that allow customers to originate, terminate or direct communications. The first requirement is expeditiously to isolate and enable the government to intercept all messages in the carrier's control to or from the equipment, facilities or services of a subscriber, concurrently with the messages' transmission, or at any later time acceptable to the government.

The second requirement is expeditiously to isolate and enable the government to access reasonably available call identifying information about the origin and destination of communications. Access must be provided in such a manner that the information may be associated with the communication to which it pertains and is provided to the government before, during or immediately after the message's transmission to or from the subscriber, or at any later time acceptable to the government. Call identifying information obtained by pen register and trap and trace devices may not include information disclosing the physical location of the subscriber sending or receiving the message, except to the extent that location is indicated by the phone number.

The third requirement is to make intercepted messages and call identifying information available to government so they may be transmitted over lines or facilities leased or procured by law enforcement to a location away from the carrier's premises.

The final requirement is to meet these requirements with a minimum of interference with the subscriber's service and in such a way that protects the privacy or messages and call identifying information that are not targeted by electronic surveillance orders, and that maintains the confidentiality of the government's wiretaps.

Subsection (b) limits the scope of the assistance requirements in several important ways. First, law enforcement agencies are not permitted to require the specific design of systems or features, nor prohibit adoption of any such design, by wire or electronic communication service providers or equipment manufacturers. The legislation leaves it to industry to decide how to comply. A carrier need not insure that each individual component of its network or system complies with the requirements so long as each communications session can be intercepted at some point.

Second, the capability requirements only apply to those services or facilities that enable a subscriber to make, receive or direct calls. They do not apply to information services, such as electronic mail providers, on-line services providers, such as CompuServe, Prodigy, America On line or Mead Data, or commercial Internet providers. Nor do they apply to services merely supporting the transport or switching of communications for the sole purposes of interconnecting carriers or private networks. Thus, a carrier providing a customer with a service or facility that allows the customer to obtain access to a publicly switched network is responsible for complying with the capability requirements. On the other hand, for communications handled by multiple carriers, a carrier that does not originate or terminate the message, but merely interconnects two other carriers, are not subject to the requirements for the interconnection part of its facilities.

Finally, telecommunications carriers have no responsibility to decrypt encrypted communications that are the subject of court-or-

dered wiretaps, unless the carrier provided the encryption and can decrypt it. This obligation is consistent with the obligation to furnish all necessary assistance under 18 U.S.C. Section 2518(4). Nothing in this paragraph would prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access.

Subsection (c) allows a carrier, in emergency or exigent circumstances, to fulfill its obligation to deliver communications to law enforcement under the third capability requirement by allowing monitoring on the carrier's premises.

Subsection (d), entitled "Mobile Service Assistance Requirement," addresses the responsibility of the carrier who can no longer deliver a message or call identifying information to law enforcement because the subscriber, the message and the call identifying information have left the carrier's service area. In such a case, the carrier that had the assistance responsibility is not required to continue providing the government with the message content of call identifying information, but must notify the government which carrier or service provider has subsequently picked up the message or call identifying information and begun serving the subscriber, subject to limitations on disclosing location information as described in section 2602(a).

Section 2603, entitled "Notice of capacity requirements," places the burden on the government to estimate its capacity needs and to do so in a cost-conscious manner, while also providing carriers with a "safe harbor" for capacity. Subsection (a) requires the Attorney General, within one year of enactment, to publish in the Federal Register and provide to appropriate industry associations and standards bodies notices of both the maximum capacity and the initial capacity required to accommodate all intercepts, pen registers, and trap and trace devices the government (including federal, state and local law enforcement) expects to operate simultaneously.

The maximum capacity relates to the greatest number of intercepts a particular switch or system must be capable of implementing simultaneously. The initial capacity relates to the number of intercepts the government will need to operate upon the date that is four years after enactment.

The Attorney General is directed to develop the notice after consultation with local and state law enforcement authorities and the carriers, equipment manufacturers and providers of support services. The Attorney General is given flexibility in determining the form of the notice. For example, the notice may be in the form of a specific number for a particular geographic area, or a generally applicable formula based on the number of subscribers served by a carrier.

Subsection (b) provides that telecommunications carriers must ensure that, within three years after publication of the notice, or within four years after enactment, whichever is longer, they have the maximum capacity and the initial capacity to execute all electronic surveillance orders. If the Attorney General publishes the first capacity notices before the statutory time of one year has elapsed, compliance by carriers must be achieved at the same time as the effective date in Section 2 of this Act. In the event the Attorney General publishes the notices after the statutory time limit, carriers will have three years thereafter to comply, which time period will fall after the effective date in Section 2 of this Act.

Subsection (c) requires the Attorney General periodically to give telecommunications carriers notice of any necessary increases in maximum capacity. Carriers will have at least three years, and up to any amount of

time beyond three years agreed to by the Attorney General, to comply with the increased maximum capacity requirements.

Section 2604 protects systems security and integrity by requiring that any electronic surveillance effected within a carrier's switching premises be activated only with intervention by an employee of the carrier. The switching premises include central offices and mobile telephone switching offices (MTSOs).

This makes clear that government agencies do not have the authority to activate remotely interceptions within the premises of a telecommunications carrier. All executions of court orders or authorizations requiring access to the switching facilities will be made through individuals authorized and designated by the telecommunications carrier. Activation of interception orders or authorizations originating in local loop wiring or cabling can be effected by government personnel or by individuals designated by the telecommunications carrier, depending upon the amount of assistance the government requires.

Section 2605 requires a telecommunications carrier to consult with its own equipment manufacturers and support service providers to identify those services or equipment to which modifications must be made for the carriers to comply with the capability requirements. Manufacturers and support services providers are required to make available to their customers who are telecommunications carriers the necessary modifications on a reasonably timely basis and at a reasonable charge.

These responsibilities of the manufacturers and support services providers make clear that they have a critical role in ensuring that lawful interceptions are not thwarted. Without their assistance, telecommunications carriers likely could not comply with the capability requirements.

Section 2606 establishes a mechanism for implementation of the capability requirements that defers, in the first instance, to industry standards organizations. Subsection (a) directs the Attorney General and other law enforcement agencies to consult with associations and standard-setting bodies of the telecommunications industry. Carriers, manufacturers and support service providers will have a "safe harbor" and be considered in compliance with the capability requirements if they comply with publicly available technical requirements or standards designed in good faith to implement the assistance requirements.

This section states affirmatively that the absence of standards will not preclude carriers, manufacturers or support service providers from deploying a technology or service, but they must still comply with the assistance requirements.

Subsection (b) provides a forum at the Federal Communications Commission in the event a dispute arises over the technical requirements or standards. Anyone can petition the FCC to establish technical requirements or standards, if none exist, or challenge any such requirements or standards issued by industry associations or bodies under this section. In taking any action under this section, the FCC is directed to protect privacy and security of communications that are not the targets of court-ordered electronic surveillance and to serve the policy of the United States to encourage the provision of new technologies and services to the public.

If an industry technical requirement or standard is set aside or supplanted by the FCC, the FCC is required to consult with the Attorney General and establish a reasonable time and conditions for compliance with and the transition to any new standard. The FCC

may also define the assistance obligations of the telecommunications carriers during this transition period.

Subsection (c) gives telecommunications carriers an additional two years to achieve compliance with the Capability Requirements beyond the four years provided in Section 2 of the Act, if they petition for, and the FCC grants, an extension. The FCC may grant a petition for relief from compliance with the Capability Requirements for up to two years in circumstances where the carrier can show that compliance with those requirements is not reasonably achievable through application of technology available within the four year compliance period. The Attorney General will reimburse the carrier for any necessary modifications made during the extension period.

Any extension granted under this subsection applies only to that part of the carrier's business on which the feature or service at issue is used.

Section 2607 provides for enforcement of the Act by the courts. Subsection (a) provides that a court may order telecommunications carriers, equipment manufacturers and support service providers to comply forthwith with the requirements of the Act in circumstances where an electronic surveillance order or authorization has been issued but cannot be effected because a carrier has failed to comply with the requirements of the Act. This provision complements the existing requirement in 18 U.S.C. §2518(4) that an order authorizing electronic surveillance may direct that providers of wire or electronic communications services or any other person . . . furnish forthwith all information, facilities, and technical assistance necessary to accomplish the interception."

Subsection (b) authorizes the Attorney General, in the absence of a particular electronic surveillance order or authorization, to apply to an appropriate United States Court for an enforcement order directing a telecommunications carriers, equipment manufacturers and support services provider to comply with the Act. In order to avoid disparate enforcement actions throughout the country which could be burdensome for telecommunications carriers, this authority is vested in the Attorney General of the United States through the Department of Justice and the Offices of the various United States Attorneys.

Subsection (c) places limitations on the court's authority to issue enforcement orders. First, the court must find that law enforcement has no alternatives reasonably available for implementing the order through use of other technologies or by serving the order on another carrier or service provider. Essentially, the court must find that law enforcement is seeking to conduct its interception at the best, or most reasonable, place for such interception.

Second, the court must find that compliance with the requirements of the Act are reasonably achievable through application of available technology, or would have been reasonably achievable if timely action had been taken. Of necessity, a determination of "reasonably achievable" will involve a consideration of economic factors. This limitation is intended to excuse a failure to comply with the Capability Requirements or capacity notices where the total cost of compliance is wholly out of proportion to the usefulness of achieving compliance for a particular type or category of services or features. This subsection recognizes that, in certain circumstances, telecommunications carriers may deploy features or services even though they are not in compliance with the requirements of this Act.

In the event that either of these standards is not met, the court may not issue an enforcement order and the carrier may proceed with deployment, or with continued offering to the public, of the feature or service at issue.

Subsection (d) requires a court upon issuance of an enforcement order to set a reasonable time and conditions for complying with the order. In determining what is reasonable, the court may consider as to each party before it a number of enumerated factors.

Subsection (e) provides that an order may not be issued requiring a carrier to exceed the capacity set forth in the Attorney General's notices under section 2603.

Subsection (f) provides for a civil penalty up to \$10,000 per day for any carrier, equipment manufacturer or support service who wilfully violates the section. In setting the appropriate amount of the fine, a court may consider a number of enumerated factors, including the nature, circumstances, and extent of the violation, and, with respect to the violator, ability to pay, good faith efforts to comply in a timely manner, effect on ability to continue to do business, the degree of culpability or delay in undertaking efforts to comply, and such other matters as justice may require.

Section 2608, entitled "Reimbursement of Telecommunications Carriers" provides, in subsection (a), that the Attorney General is required to pay all reasonable costs directly associated with modifications required to comply with the Capability Requirements, either during the period of four years after enactment or during any extension period granted by the FCC. In addition, the Attorney General is required to pay such costs for expanding the carrier's facilities in the event such expansion is necessary to comply with the notices issued under section 2603 of maximum and initial capacity needed by law enforcement.

Subsection (b) authorizes the Attorney General to establish necessary regulations and procedures to reimburse carriers.

Subsection (c) provides that any dispute over costs is to be resolved by the FCC or the court from which an enforcement order is sought.

Subsection (d) provides that if appropriated funds are insufficient to satisfy the Attorney General's obligation under subsection (a) to reimburse carriers for the modifications required under section 2602 and for the capacity required under section 2603, the court may take this into account in determining whether compliance is reasonably achievable before issuing any enforcement order. The FCC may take this into account in determining whether compliance is reasonably achievable during a proceeding to extend the deadline for compliance with the Capability Requirements.

Section 2. Authorization of appropriations. This section authorizes \$500,000,000 to be appropriated for 1995 through 1998, which encompasses the four years after enactment, and thereafter any additional amounts that may be necessary to carry out the purposes of the Act.

Section 3. Effective date. This section sets the effective date for compliance with the Capability Requirements in section 2602 and the Systems Security and Integrity requirement in section 2604 as four years after the enactment. All other provisions take effect upon date of enactment.

Section 4. Reports. The Attorney General is required to report annually to Congress periodically for the five years after enactment on the monies expended under the Act. In addition, the General Accounting Office is required to report in 1996 and 1998 on costs of compliance with this Act.

Section 5. Cordless telephones. The Electronic Communications Privacy Act (ECPA), which amended the wiretap statute in 1986, exempted from the protection of the Act "the radio portion of a cordless telephone that is transmitted between the cordless telephone handset and the base unit." 18 U.S.C. §2510 (1) & (12). In view of the current ubiquitous use of such phones and the expectation that such calls are protected just like other calls, Sen. Leahy's 1991 Privacy and Technology Task Force Report ("Task Force") recommended that privacy protection be extended to cordless phones, provided an exception for unintentional or accidental party interception was preserved.

Consistent with the Task Force's recommendations and the Administration's digital telephony proposal, the bill would delete the exceptions for cordless phones and impose a penalty of up to \$500 for intentionally intercepting such communications.

Sections 6 & 7. Radio-based communications. ECPA does not protect communications that are "readily accessible to the general public," which includes radio communications, unless they fit into one of the five specified categories. These excepted categories enjoy protection because they usually are not susceptible to interception by the general public.

Consistent with the Task Force's recommendations and the Administration's digital telephony proposal, the bill would add "electronic communication" as a category of radio communication covered by the wiretap statute. This would provide protection for all forms of electronic communications, including data, even when they may be transmitted by radio.

The bill also amends the penalty provision to treat communications using modulation techniques in the same fashion as those where encryption has been employed to secure communications privacy. This paragraph refers to spread spectrum radio communications, which usually involve the transmission of a signal on different frequencies where the receiving station must possess the necessary algorithm in order to reassemble the signal.

Section 8. Technical correction. The wiretap law permits interception of wire communications by a wire or electronic service provider in the normal course of business to render services or protect rights or property. The bill would make a technical correction and expand the exception to include electronic communications.

Section 9. Clone phones. This section amends the Counterfeit Access Device law to criminalize the use of cellular phones that are altered, or "cloned," to allow free riding on the cellular phone system. Specifically, this section prohibits the use of an altered telecommunications instrument, or a scanning receiver, hardware or software, to obtain unauthorized access to telecommunications services. A scanning receiver is defined as a device used to intercept illegally wire, oral or electronic communications. The penalty for violating this new section is imprisonment for up to fifteen years and a fine of the greater of \$50,000 or twice the value obtained by the offense.

Section 10. Transactional data. Recognizing that transactional records from on-line communication systems reveal more than telephone toll records or mail covers, subsection (a) eliminates the use of a subpoena by law enforcement to obtain from a provider or electronic communication services the addresses on electronic messages. In order for law enforcement to obtain such information, a court order is required.

This section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a sub-

S. 2330

At the request of Mr. ROCKEFELLER, the names of the Senator from New York [Mr. MOYNIHAN], the Senator from Massachusetts [Mr. KENNEDY], the Senator from Washington [Mrs. MURRAY], the Senator from Kansas [Mr. DOLE], and the Senator from Delaware [Mr. BIDEN] were added as cosponsors of S. 2330, a bill to amend title 38, United States Code, to provide that undiagnosed illnesses constitute diseases for purposes of entitlement of veterans to disability compensation for service-connected diseases, and for other purposes.

AMENDMENTS SUBMITTED

DEPARTMENT OF DEFENSE APPROPRIATIONS ACT FOR FISCAL YEAR 1995

BUMPERS (AND OTHERS)
AMENDMENT NO. 2481

Mr. BUMPERS (for himself, Mr. CONRAD, Mr. LEAHY, Mr. FEINGOLD, Mr. KOHL, Mr. WELLSTONE, and Mr. SIMON) proposed an amendment to the bill (H.R. 4650) making appropriations for the Department of Defense for the fiscal year ending September 30, 1995, and for other purposes; as follows:

On page 37, line 7, in lieu of the matter proposed to be inserted, add the following: "\$12,111,511,000, to remain available for obligation until September 30, 1996: Provided that of the funds appropriated in this paragraph, none may be obligated or expended for parts or other components associated with the acquisition of Milstar satellites numbers 5 and 6: Provided further that \$61,595,000 shall be used to develop an advanced EHF military satellite communications system."

BOXER (AND OTHERS)
AMENDMENT NO. 2482

Mr. INOUE (for Mrs. BOXER, for herself, Mr. STEVENS, and Mr. INOUE) proposed an amendment to the bill H.R. 4650, supra; as follows:

On page 142, between lines 7 and 8, insert the following:

SEC. 8121. (a) STUDY.—The Secretary of Defense shall conduct a study of the receipt of benefits under the Food Stamp Act of 1977 (7 U.S.C. 2011 et seq.) by the members of the Armed Forces. The study shall include the following elements:

- (1) The number of members of the Armed Forces who are eligible to receive benefits under that Act.
- (2) The number of such members who receive benefits under that Act.
- (3) The location by State and region of the members referred to in paragraphs (1) and (2).
- (4) An estimate of the cost of raising the rate of basic pay of members of the Armed Forces to a rate at which such members would no longer be eligible to receive benefits under that Act.

(b) REPORT.—The Secretary shall submit to Congress a report on the study required under subsection (b) not later than 180 days after the date of the enactment of this Act.

poena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement. Under the intermediate standard, law enforcement must show facts which establish why such records are relevant and material to an ongoing criminal investigation.

Law enforcement could still use a subpoena to obtain the name, billing address, and length of service of a subscriber to or customer of such service and the type of services the subscriber or customer utilized.

Subsection (b) requires government agencies installing and using pen register devices to use, when reasonably available, technology that restricts the information captured by such device to the dialling or signaling information necessary to direct or process a call, excluding any further communications conducted through the use of dialled digits that would otherwise be captured.

ADDITIONAL COSPONSORS

S. 993

At the request of Mr. KEMP THORNE, the names of the Senator from Arkansas [Mr. BUMPERS] and the Senator from Michigan [Mr. LEVIN] were added as cosponsors of S. 993, a bill to end the practice of imposing unfunded Federal mandates on States and local governments and to ensure that the Federal Government pays the costs incurred by those governments in complying with certain requirements under Federal statutes and regulations.

S. 1417

At the request of Mr. LIEBERMAN, the name of the Senator from New York [Mr. MOYNIHAN] was added as a cosponsor of S. 1412, a bill to amend title 13, United States Code, to require that any data relating to the incidence of poverty, produced or published by the Secretary of Commerce for subnational areas is corrected for differences in the cost of living in those areas.

S. 1513

At the request of Mr. KENNEDY, the names of the Senator from Michigan [Mr. RIEGLE] and the Senator from Rhode Island [Mr. CHAFEE] were added as cosponsors of S. 1513, a bill entitled "Improving America's Schools Act of 1993."

S. 1541

At the request of Mr. COVERDELL, the name of the Senator from Mississippi [Mr. LOTT] was added as a cosponsor of S. 1541, a bill to provide that a non-governmental person may use a private express carriage of certain letters and packets without being penalized by the Postal Service, and for other purposes.

S. 1822

At the request of Mr. DANFORTH, the name of the Senator from Mississippi [Mr. LOTT] was added as a cosponsor of S. 1822, a bill to foster the further development of the Nation's telecommunications infrastructure and protection of the public interest, and for other purposes.

S. 1898

At the request of Mr. RIEGLE, the name of the Senator from Tennessee

[Mr. MATHEWS] was added as a cosponsor of S. 1898, a bill to amend the Internal Revenue Code of 1986 to make permanent the section 170(e)(5) rules pertaining to gifts of publicly traded stock to certain private foundations, and for other purposes.

S. 1976

At the request of Mr. DODD, the names of the Senator from Texas [Mrs. HUTCHISON] and the Senator from North Dakota [Mr. CONRAD] were added as cosponsors of S. 1976, a bill to amend the Securities Exchange Act of 1934 to establish a filing deadline and to provide certain safeguards to ensure that the interests of investors are well protected under the implied private action provisions of the act.

S. 2192

At the request of Mr. BENNETT, the names of the Senator from Delaware [Mr. ROTH] and the Senator from Washington [Mrs. MURRAY] were added as cosponsors of S. 2192, a bill to amend the Securities Exchange Act of 1934 with respect to the extension of unlisted trading privileges for corporate securities, and for other purposes.

S. 2255

At the request of Mr. GORTON, the name of the Senator from Alaska [Mr. STEVENS] was added as a cosponsor of S. 2255, a bill to amend the Budget Enforcement Act of 1990 to establish a new budget point of order against any amendment, bill, or conference report that directs increased revenues from additional taxation of Social Security or railroad retirement benefits to a fund other than the Social Security trust fund or the Social Security equivalent benefit account.

S. 2312

At the request of Mr. DASCHLE, the names of the Senator from Arkansas [Mr. PRYOR], the Senator from Mississippi [Mr. COCHRAN], the Senator from North Dakota [Mr. CONRAD], the Senator from Iowa [Mr. GRASSLEY], the Senator from Montana [Mr. BAUCUS], the Senator from Nebraska [Mr. KERREY], the Senator from North Dakota [Mr. DORGAN], the Senator from Idaho [Mr. CRAIG], the Senator from Pennsylvania [Mr. WOFFORD], the Senator from Iowa [Mr. HARKIN], the Senator from Illinois [Mr. SIMON], the Senator from Wisconsin [Mr. KOHL], the Senator from Montana [Mr. BURNS], the Senator from Wisconsin [Mr. FEINGOLD], the Senator from Oklahoma [Mr. BOREN], the Senator from Kentucky [Mr. MCCONNELL], the Senator from Alabama [Mr. SHELBY], the Senator from South Dakota [Mr. PRESLER], the Senator from Missouri [Mr. BOND], the Senator from Alabama [Mr. HEFLIN], and the Senator from Mississippi [Mr. LOTT] were added as cosponsors of S. 2312, a bill to maintain the ability of U.S. agriculture to remain viable and competitive in domestic and international markets, to meet the food and fiber needs of United States and international consumers, and for other purposes.