LAW
KF
31
.J8
1986
cop. 2

99TH CONGRESS } SENATE { REPORT 99-541

Calendar No. 1064

ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

OCTOBER 17 (legislative day, OCTOBER 10), 1986.—Ordered to be printed

Mr. THURMOND, from the Committee on the Judiciary, submitted the following

REPORT

[To accompany S. 2575]

The Committee on the Judiciary, to which was referred the bill (S. 2575) having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE

The Electronic Communications Privacy Act amends title III of the Omnibus Crime Control and Safe Streets Act of 1968—the Federal wiretap law—to protect against the unauthorized interception of electronic communications. The bill amends the 1968 law to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.

When the Framers of the Constitution acted to guard against the arbitrary use of Government power to maintain surveillance over citizens, there were limited methods of intrusion into the "houses,

papers, and effects" protected by the fourth amendment. During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such intrusions.

The telephone is the most obvious example. Its widespread use made it technologically possible to intercept the communications of citizens without entering homes or other private places. When the issue of Government wiretapping first came before the Supreme Court in *Olmstead* v. *United States,* 277 U.S. 438 (1928), the Court held that wiretapping did not violate the fourth amendment, since there was no searching, no seizure of anything tangible, and no physical trespass.

Today, the *Olmstead* case is often remembered more for Justice Brandeis' prescient dissent than for its holding. Justice Brandeis predicted:

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home . . . Can it be that the Constitution affords no protection against such invasions of individual security?

Forty years later, the Supreme Court accepted Justice Brandeis' logic in *Katz* v. *United States,* 389 U.S. 347 (1967), holding that the fourth amendment applies to Government interception of a telephone conversation. At the same time, the Court extended fourth amendment protection to electronic eavesdropping on oral conversations in *Berger* v. *New York,* 388 U.S. 41 (1967).

Congress responded in a comprehensive fashion by authorizing Government interception, under carefully subscribed circumstances in title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510 et seq. Title III is the primary law protecting the security and privacy of business and personal communications in the United States today. Its regimen for protecting the privacy of voice communications is expressly limited to the unauthorized aural interception of wire or oral communications. It only applies where the contents of a communication can be overheard and understood by the human ear. See *United States* v. *New York Telephone Company,* 434 U.S. 159, 167 (1977). Furthermore, existing title III applies only to interceptions of communications sent via common carriers. 18 U.S.C. 2510(10).

As Senator Leahy said when he introducted S. 2575 with Senator Mathias, the existing law is "hopelessly out of date." Congressional Record, June 19, 1986. It has not kept pace with the development of communications and computer technology. Nor has it kept pace with changes in the structure of the telecommunications industry.

Today we have large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing.[1] A phone call can be carried by wire, by microwave or fiber optics. It can be transmitted in the form of digitized voice, data or video. Since the divestiture of

[1] These new forms of telecommunications and computer technology are described in the Glossary below.

AT&T and deregulation, many different companies, not just common carriers, offer a wide variety of telephone and other communications services. It does not make sense that a phone call transmitted via common carrier is protected by the current federal wiretap statute, while the same phone call transmitted via a private telephone network such as those used by many major U.S. corporations today, would not be covered by the statute.

These tremendous advances in telecommunications and computer technologies have carried with them comparable technological advances in surveillance devices and techniques. Electronic hardware making it possible for overzealous law enforcement agencies, industrial spies and private parties to intercept the personal or proprietary communications of others are readily available in the American market today.

Title I of the Electronic Communications Privacy Act addresses the interception of wire, oral and electronic communications. It amends existing chapter 119 of title 18 to bring it in line with technological developments and changes in the structure of the telecommunications industry.

The Committee also recognizes that computers are used extensively today for the storage and processing of information. With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. For example, physicians and hospitals maintain medical files in offsite data banks, businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services. These services as well as the providers of electronic mail create electronic copies of private correspondence for later reference. This information is processed for the benefit of the user but often it is maintained for approximately 3 months to ensure system integrity. For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection. See *United States* v. *Miller,* 425 U.S. 435 (1976) (customer has no standing to contest disclosure of his bank records). Thus, the information may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties. The provider of these services can do little under current law to resist unauthorized access to communications.

Title II of S. 2575 addresses access to stored wire and electronic communications and transactional records. It is modeled after the Right to Financial Privacy Act, 12 U.S.C. 3401 et seq. to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs.

Title III of the bill addresses pen registers and trap and trace devices.

II. History

In 1984, Senator Leahy asked the Attorney General whether he believed interceptions of electronic mail and computer-to-computer communications were covered by the Federal wiretap law. The

Criminal Division of the Justice Department responded that Federal law protects electronic communications against unauthorized acquisition only where a reasonable expectation of privacy exists. Underscoring the need for this legislation, the Department concluded:

> In this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions such as [whether there does or does not exist a reasonable expectation of privacy] are not always clear or obvious.

Senator Leahy's letter and the Justice Department's response mark the beginning of this legislation. The Subcommittee on Patents, Copyrights and Trademarks chaired by Senator Mathias, held hearings in the 98th Congress. See, Hearing before the Subcommittee on Patents, Copyrights and Trademarks of the Committee on the Judiciary on Privacy and Electronic Communications, September 12, 1984, S. Hrg. 98–1266.

The product of that hearing and subsequent discussions with the Department of Justice and private groups interested in promoting communications privacy, while protecting legitimate law enforcement needs and promoting technological innovation, was S. 1667, the Electronic Communications Privacy Act of 1985. Senators Leahy and Mathias introduced that bill on September 19, 1985. On the same day, Congressmen Kastenmeier and Moorhead, the Chairman and Ranking Minority Member of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice introduced an identical bill, H.R. 3378.

In October 1985, the Office of Technology Assessment issued a report entitled "Electronic Surveillance and Civil Liberties." That study concluded that current legal protections for electronic mail are "weak, ambiguous, or non-existent," and that "electronic mail remains legally as well as technically vulnerable to unauthorized surveillance." "Federal Government Information Technology: Electronic Surveillance and Civil Liberties" (Washington, D.C.: U.S. Congress, Office of Technology Assessment, OTA–CIT–293, October 1985).

The Subcommittee on Patents, Copyrights and Trademarks held a hearing on S. 1667 on November 13, 1985. Testimony was received from interested individuals and groups, including representatives of the telephone industry, the electronic mail industry, and the software and service industries. Representatives of the Department of Justice presented their views, and the subcommittee also received testimony from the American Civil Liberties Union and elicited technical information from the Institute of Electrical and Electronics Engineers.

As a result of those hearings, S. 1667 was superseded by a new bill to reflect the concerns raised by some of these groups, particularly the Department of Justice and radio hobbyists. On June 19, 1986, Senator Leahy, joined by Senator Mathias, introduced S. 2575.

On August 12, 1986, the Judiciary Committee Subcommittee on Patents, Copyrights and Trademarks favorably reported S. 2575, as amended, to the full Committee by voice vote.

On September 19, 1986, Senators Leahy and Mathias and Chairman Thurmond offered an amendment in the nature of a substitute to S. 2575. The Committee voted unanimously to favorably report the Electronic Communications Privacy Act of 1986, as amended, to the full Senate.

III. Statement

A letter sent by first class mail is afforded a high level of protection against unauthorized opening by a combination of constitutional provisions, case law, and U.S. Postal Service statutes and regulations. Voice communications transmitted via common carrier are protected by title III of the Omnibus Crime Control and Safe Streets Act of 1968.

But there are no comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology. This is so, even though American citizens and American businesses are using these new forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services.

This gap results in legal uncertainty. It may unnecessarily discourage potential customers from using innovative communications systems. It probably encourages unauthorized users to obtain access to communications to which they are not a party. It may discourage American businesses from developing new innovative forms of telecommunications and computer technology. The lack of clear standards may expose law enforcement officers to liability and may endanger the admissibility of evidence.

Most importantly, the law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.

The Committee believes that S. 2575, te Electronic Communications Privacy Act of 1986, represents a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies.

The Justice Department strongly supports S. 2575 because it strengthens the current wiretap law from a law enforcement perspective. Specifically, it expands the list of felonies for which a voice wiretap order may be issued and the list of Justice Department officials who may apply for a court order to place a wiretap. The bill also includes provisions making it easier for law enforcement officials to deal with a target who repeatedly changes telephones to thwart interception of his communications and creates criminal penalties for those who notify a target of a wiretap in order to obstruct it. These provisions will be particularly helpful to the Justice Department in its fight against drug trafficking.

The organizations and individual corporations named below also support the principles embodied in the legislation.

Organizations: Electronic Mail Assoc.; ADAPSO; Telocator Network of America; Cellular Telecommunications Industry Assoc.;

ACLU; National Association of Manufacturers (NAM); U.S. Chamber of Commerce; National Association of Broadcasters (NAB); National Cable Television Assoc. (NCTA); National Association of Business & Educational Radio (NABER); CBEMA; U.S. Telephone Assoc.; Videotext Industry Assoc.; Information Industry Assoc.; Electronic Funds Transfer Assoc.; Radio and Television News Directors Assoc.; Association of American Railroads; Institute of Electrical and Electronics Engineers (IEEE); Direct Marketing Association; Utilities Telecommunications Council; and Associated Credit Bureaus, Inc.

Corporations: AT&T; General Electric; IBM; GTE; EDS; ITT; MCI; CBS; ABC; NBC; Tandy Corp. (Radio Shack); Trintex; Equifax; TRW; Source Telecomputing Corporation; Chase Manhattan Bank; Motorola; Ameritech; Bell Atlantic; Bell South; Southwestern Bell; NYNEX; Pacific Telesis; US West; and Associated Credit Services, Inc.

A few points in the development of the Electronic Communications Privacy Act of 1986 should be noted here. After Senators Leahy and Mathias introduced the bill in June 1986, S. 2575 was referred to the Subcommittee on Patents, Copyrights and Trademarks. During the subcommittee markup session held on August 12, 1986, the bill was further amended to clarify certain provisions.

At the request of the FCC, in response to the recent Captain Midnight incident, in which an individual in Florida interfered with the transmission of an HBO program being relayed by satellite, the subcommittee included in the bill language to address deliberate or malicious interference with satellite transmissions. It also added to title III of the bill related to installation and use of pen registers, procedural requirements for orders to use "trap and trace" devices.

In order to underscore that the inadvertent reception of a protected communication is not a crime, the subcommittee changed the state of mind requirement under title III of the Omnibus Crime Control and Safe Streets Act of 1968 from "willful" to "intentional." This change in the law addresses the concerns of radio scanners that in the course of scanning radio frequencies in order to receive public communications, one could inadvertently tune through a protected communication like a cellular telephone call. This provision makes clear that the inadvertent interception of a protected communication is not unlawful under this Act.

During subcommittee consideration, Senators Laxalt, Grassley, DeConcini and Simpson expressed concerns about the bill's penalty structure for the interception of certain satellite transmissions by home viewers. Senators Leahy and Mathias agreed that those concerns would be addressed during Committee consideration of the Electronic Communications Privacy Act.

The Leahy-Mathias-Thurmond substitute for S. 2575, which was offered when the full Committee considered this legislation, incorporated an amendment offered by Senator Grassley. Senators Laxalt, McConnell, Simpson and Denton cosponsored Senator Grassley's amendment.

Senator Grassley's amendment modifies the criminal penalties and civil liability provisions of chapter 119 of title 18 of the United States Code so that there is a two-track, tiered penalty structure for home viewing of private satellite transmissions when the con-

duct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain.

In a public action, under the Grassley amendment, a first offender would be subject to a suit by the Government for injunctive relief. If injunctive relief is granted, one who violates the injunction would be subject to the full panoply of enforcement mechanisms within the court's existing authority, including criminal and civil contempt. Second and subsequent offenses carry a mandatory $50 civil fine for each violation. The term "violation" in this context refers to each viewing of a private video communication.

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

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

The substitute amendment also incorporated Senator Simon's amendment. Senator Simon had expressed concern that the Electronic Communications Privacy Act's penalties were too severe for the first offender, who without an unlawful or financial purpose, intercepts a cellular telephone call or certain radio communications related to news-gathering.

Senator Simon's amendment reduces the penalty for such an interception of an unencrypted, unscrambled cellular telephone call to a $500 criminal fine. Unencrypted, unscrambled radio communications transmitted on frequencies allocated under subpart D of part 74 of the FCC rules are treated like private satellite video communications are under Senator Grassley's amendment.

Scanning enthusiasts have argued to the Committee that the mere monitoring of cellular telepnone calls should not be illegal. That argument ignores three important realities. First, Congress, in passing the 1968 wiretap law already made willful monitoring of such telephone calls illegal when at least part of the conversation is carried by wire. Second, unlike many signals which are more commonly scanned, the design of the cellular telepnone system makes the intentional monitoring of specific calls more difficult be-

cause they are handed off among cells. The Committee is not convinced that these arguments overcome the need for protection of privacy interests.

It has been suggested that the Federal Communications Commission consider labeling requirements on cellular telephnones, radio scanning equipment and private satellite video communications. The Commission might consider the feasibility of requiring that cellular telephones be labeled to indicate that cellular calls are radio-based communications, and as such, portions of the communication may be intercepted by available scanning equipment and of requiring that scanning equipment be labeled to indicate that the intentional interception of protected communications could be a Federal criminal violation. Finally, the Commission might consider the feasibility of requiring those who transmit private satellite video communications to periodically transmit a crawl across the bottom of the screen indicating that such communications are protected.

IV. Glossary

For reference, some of the new telecommunications and computer technologies referred to in the Electronic Communications Privacy Act of 1986 and this report are described briefly below. Treatment of these and other technologies under current law is discussed in the House Report to its companion measure, H.R. 4952. *See* House Report 99-647.

ELECTRONIC MAIL

Electronic mail is a form of communication by which private correspondence is transmitted over public and private telephone lines. In its most common form, messages are typed into a computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic mail company. If the intended addressee subscribes to the service, the message is stored by the company's computer "mail box" until the subscriber calls the company to retrieve its mail, which is then routed over the telephone system to the recipient's computer. If the addressee is not a subscriber to the service, the electronic mail company can put the message onto paper and then deposit it in the normal postal system.

Electronic mail systems may be available for public use or may be proprietary, such as systems operated by private companies for internal correspondence.

COMPUTER-TO-COMPUTER COMMUNICATIONS

Common computer-to-computer communications include the transmission of financial records or funds transfers among financial institutions, medical records between hospitals and/or physicians' offices, and the transmission of proprietary data among the various offices of a company.

ELECTRONIC BULLETIN BOARDS

Electronic "bulletin boards" are communications networks created by computer users for the transfer of information among com-

puters. These may take the form of proprietary systems or they may be noncommercial systems operating among computer users who share special interests. These noncommercial systems may involve fees covering operating costs and may require special "passwords" which restrict entry to the system. These bulletin boards may be public or semi-public in nature, depending on the degree of privacy sought by users, operators or organizers of such systems.

MICROWAVE

Microwave consists of extremely high frequency radio waves transmitted point-to-point on line-of-sight paths between antennas located on towers or building tops (in terrestrial microwave systems) and between satellites and earth station "dish" antennas (in satellite-based systems).

CELLULAR TELEPHONES

In 1981 the Federal Communications Commission approved the use of cellular telephone services. This technology uses both radio transmission and wire to make "portable" telephone service available in a car, a briefcase, or in rural areas not reached by telephone wire.

In a cellular radiotelephone system, large service areas are divided into honeycomb-shaped segments or "cells"—each of which is equipped with a low-power transmitter or base station which can receive and radiate messages within its parameters. When a caller dials a number on a cellular telephone, a transceiver sends signals over the air on a radio frequency to a cell site. From there the signal travels over phone lines or a microwave to a computerized mobile telephone switching office ("MTSO") or station. The MTSO automatically and inaudibly switches the conversation from one base station and one frequency to another as the portable telephone, typically in a motor vehicle, moves from cell to cell.

Cellular technology, because it is more complex, is more difficult to intercept than traditional mobile telephones; it is, however, more accessible than microwave transmissions. Cellular telephone calls can be intercepted by either sophisticated scanners designed for that purpose, or by regular radio scanners modified to intercept cellular calls.

CORDLESS TELEPHONES

A cordless telephone consists of a handset and a base unit wired to a landline and a household/business electrical current. A communication is transmitted from the handset to the base unit by AM or FM radio signals. From the base unit the communication is transmitted over wire, the same as a regular telephone call. The radio portions of these telephone calls can be intercepted with relative ease using standard AM radios.

ELECTRONIC PAGERS

Electronic pagers are radio activated devises through which a user is notified of another's attempt to contact the carrier of the portable paging unit. These are in wide use among persons who are away from their homes or offices—or, more precisely, away from

telephones or two-way radios—yet still need to be reachable by others.

Pagers take on one of three basic forms: "tone only," "display" and "tone and voice pagers." The "tone only" device emits a "beep" or other signal to inform the user that a message is waiting, and where that message can be retrieved by the user's making a phone call to a predetermined number (usually an office or answering service). "Display" pagers are equipped with screens that can display visual messages, usually the telephone number of the person seeking to reach the person being paged. The party seeking to make contact with the user is instructed to provide a message, usually by pushing the buttons of a touch-tone telephone; this message is stored by the paging company's computer until it can be transmitted to the user's pager, where the message can then be read directly by the user, obviating the need for the user to make a telephone call to retrieve the message. The most sophisticated type of pager is the "tone and voice" model. It can receive a spoken message that the paging company's computer has taken from the party seeking to contact the unit's user. After the beep tone is made, the device "repeats" the recorded message. This requires that a radio signal containing voice communications be sent from the paging company's base to the mobile unit.

PEN REGISTERS/TRAP AND TRACE DEVICES

Pen registers are devices that record the telephone numbers to which calls have been placed from a particular telephone. These capture no part of an actual telephone conversation, but merely the electronic switching signals that connect two telephones. The same holds true for trap and trace devices, which record the numbers of telephones from which calls have been placed to a particular telephone.

ELECTRONIC TRACKING DEVICES (TRANSPONDERS)

These are one-way radio communication devices that emit a signal on a specific radio frequency. This signal can be received by special tracking equipment, and allows the user to trace the geographical location of the transponder. Such "homing" devices are used by law enforcement personnel to keep track of the physical whereabouts of the sending unit, which might be placed in an automobile, on a person, or in some other item.

REMOTE COMPUTER SERVICES

In the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data in-house on the user's own computer or on someone else's equipment. Over the years, remote computer service companies have developed to provide sophisticated and convenient computing services to subscribers and customers from remote facilities. Today businesses of all sizes—hospitals, banks and many others—use remote computing services for computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information

supplied by the subscriber or customer. Data is most often transmitted between these services and their customers by means of electronic communications.

V. Section-by-Section Analysis

Section 1 provides that the short title of the bill is the "Electronic Communications Privacy Act of 1986."

TITLE I—INTERCEPTION OF COMMUNICATIONS AND RELATED MATTERS

Under current law, the interception of wire and oral communications are governed by chapter 119 of title 18 (18 U.S.C. 2510 et seq.). Title I of the Electronic Communications Privacy Act expands chapter 119 to take into account modern advances in electronic telecommunications and computer technology.

Section 101—Federal penalties for the interception of communications

Definitions for terms used in chapter 119 and new chapter 121 of title 18 are set out in section 101 of the bill. This section also describes conduct which is not unlawful under this Act and modifies the penalties set out in existing section 2511 of title 18. It provides that the remedies in chapter 119 are the exclusive statutory remedies for violations of this chapter. Technical amendments to chapter 119 are also included in Section 101 of the bill.

Subsection 101(a)—Definitions

Subsection 101(a) of the Electronic Communications Privacy Act sets out the definitions and amendments to definitions used in chapter 119 and new chapter 121 of title 18. Paragraph 101(a)(1) amends the definition of the term "wire communication" in subsection 2510(1) of title 18.

Subparagraph (A) amends that definition to include aural transfers. As defined in proposed subsection 2510(18) of title 18, "aural transfers" are those which include the human voice at any point between and including the points of origin and reception.

Subparagraph (B) specifies that the use of wire, cable or other similar connections for the transmission of communications includes the use of such connections in a switching station. This subparagraph makes clear that cellular communications—whether they are between two cellular telephones or between a cellular telephone and a "land line" telephone—are included in the definition of "wire communications" and are covered by the statute. As noted below, the bill distinguishes between cordless and cellular telephones.

Recognizing that since deregulation and the divestiture of AT&T, many different companies, not just common carriers, offer and use telephone and other communications services, subpargraph (C) deletes from the definition of "wire communication" the requirement that communications must be transmitted via common carrier to be covered by the federal wiretap statute.

Subparagraph (D) specifies that wire, cable or similar connections furnished or operated by any person engaged in providing or operating such facilities for the transmission of "communications

affecting interstate or foreign commerce," are within the definition of a "wire communication." This language recognizes that private networks and intra-company communications systems are common today and brings them within the protection of the statute. However, that language is not meant to suggest that the Electronic Communications Privacy Act applies to interceptions made outside the territorial United States. Like the Omnibus Crime Control and Safe Streets Act of 1968 which it revises, the Electronic Communications Privacy Act regulates only those interceptions conducted within the territorial United States.

The Senate Judiciary Committee's Subcommittee on Patents, Copyrights and Trademarks amended subparagraph (D) to specify that wire communications in storage like voice mail, remain wire communications, and are protected accordingly.

The combined effect of subparagraphs (A) through (D) is to clarify that the term "wire communication" means the transfer of a communication which includes the human voice at some point. The transfer must be made in whole or in part through the use of communication transmission facilities by the aid of wire, cable, or other like connection, including fiber optics. The facilities may be furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or he may provide or operate those facilities for the transmission of communications affecting interstate or foreign commerce.

Thus, a wire communication encompasses the whole of a voice telephone transmission even if part of the transmission is carried by fiber optic cable or by radio—as in the case of cellular telephones and long distance satellite or micowave facilities. The conversion of a voice signal to digital form for purposes of transmission does not render the communication non-wire. The term "wire communication" includes existing telephone service, and digitized communications to the extent that they contain the human voice at the point of origin, reception, or some point in between. A private telephone system established by a company whose activities affect interstate commerce, would also be covered.

It should be noted that an improperly mechanical reading of the phrase "in whole or in part * * * by the aid of wire * * *" could sweep in virtually all voice communications made with the aid of any electronic equipment, inasmuch as virtually all such equipment includes in its assembly some length of wire or the equivalent. The quoted is intended to refer to wire that carries the communication to a significant extent from the point of origin to the point of reception, even in the same building. It does not refer to wire that is found inside the terminal equipment at either end of the communication.

Subparagraph (D) specifies that the term "wire communication" does not include the radio portion of a cordless telephone communication transmitted between the cordless handset and the base unit. Because communications made on some cordless telephones can be intercepted easily with readily available technologies, such as an AM radio, it would be inappropriate to make the interception of such a communication a criminal offense. The wire portion of a cordless communication remains fully covered, however.

Section 101(a)(2) of the Electronic Communications Privacy Act amends the definition of "oral communication" in current section 2510(2) of title 18 to exclude electronic communications. There have been cases involving radio communications in which the court having determined that the radio communication was not a wire communication then analyzes it in privacy terms to determine if it is an oral communication. The bill rejects that analysis by excluding electronic communications from the definition of oral communications.

An oral communication is an utterance by a person under circumstances exhibiting an expectation that the communication is not subject to interception, under circumstances justifying such an expectation. In essence, an oral communication is one carried by sound waves, not by an electronic medium.

Section 101(a)(3) of the Electronic Communications Privacy Act amends the definition of the term "intercept" in current section 2510(4) of title 18 to cover electronic communications. The definition of "intercept" under current law is retained with respect to wire and oral communications except that the term "or other" is inserted after "aural." This amendment clarifies that it is illegal to intercept the non-voice portion of a wire communication. For example, it is illegal to intercept the data or digitized portion of a voice communication.

Subsection 101(a)(4) of the Electronic Communications Privacy Act amends existing section 2510(5) of title 18 to clarify that telephone equipment provided by the user and connected to the facilities of a service provider is not an "electronic, mechanical or other device," provided that it is used in the ordinary course of the user's business.

The Committee notes that proposed section 2510's definition of an "electronic, mechanical or other device" includes any combination of parts designed or intended for use in converting those parts into such a device or apparatus and from which such a device or apparatus may be readily assembled. The Committee also notes that section 2512, as amended by the Electronic Communications Privacy Act, prohibits the manufacture, distribution, possession, and advertising only of devices primarily useful for surreptitious interception.

Subsection 101(a)(5) of the Electronic Communications Privacy Act amends current section 2510(8) of title 18 to exclude from the definition of the term "contents," the identity of the parties or the existence of the communication. It thus distinguishes between the substance, purport or meaning of the communication and the existence of the communication or transactional records about it.

The Supreme Court has clearly indicated that the use of pen registers does not violate either chapter 119 of title 18 or the fourth amendment. Subsection 101(a)(5) of this legislation makes that policy clear. It should be read in conjunction with Title III of the Electronic Communications Privacy Act which adds new chapter 206 on pen registers and trap and trace devices to title 18. Subsection 101(a)(5) of the bill does not affect the installation or use of pen registers under the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. 1801 et. seq. Similarly, the omission of a conforming amendment to the definition of "contents" in section 705 of

title 47 is not intended to affect the current law under that section with respect to pen registers. The use of pen registers has been found not to violate section 705. See *Hodge* v. *Mountains Tel. & Telegraph Co.*, 555 F.2d 254 (9th Cir. 1977).

Subsection 101(a)(6) of the Electronic Communications Privacy Act adds to section 2510 of title 18 definitions for the terms "electronic communication," "electronic communications system," "electronic communication service," "readily accessible to the general public," "electronic storage," and "aural transfer."

An "electronic communication" is defined in proposed subsection 2510(12) of title 18 as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or a photooptical system that affects foreign or interstate commerce." The following are explicitly excluded from the definition: (A) the radio portion of a cordless telephone communication transmitted between the cordless phone handset and the base unit; (B) any wire or oral communication; (C) any communication made through a tone-only paging device; (D) any communication from a tracking device.

As a general rule, a communication is an electronic communication protected by the federal wiretap law if it is not carried by sound waves and cannot fairly be characterized as containing the human voice. Communications consisting solely of data, for example, and all communications transmitted only by radio are electronic communications. This term also includes electronic mail, digitized transmissions, and video teleconferences. Although radio communications are within the scope of the Act, the provisions of the Electronic Communications Privacy Act directed specifically to radio do not affect the applicability of section 705 of the Communications Act of 1934, as amended, to actions by members of the public.

Under proposed subsection 2510(13), the term "user" is defined as any person or entity who (A) uses an electronic communication service and (B) is duly authorized by the service provider to do so.

An "electronic communication system" is defined in proposed subsection 2510(14). Such a system encompasses any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications as well as any computer facilities or related electronic equipment for the electronic storage of such communications.

An "electronic communication service" is defined in proposed subsection 2510(15) of title 18 as a service which provides its users the ability to send or to receive wire or electronic communications. Such services can be provided through the same facilities. Existing telephone companies and electronic mail companies are providers of electronic communication services. Other services like remote computing services may also provide electronic communication services.

Radio communications "readily accessible to the general public" are defined in proposed subsection 2510(16). Radio communications are considered readily accessible to the general public unless they fit into one of five specified categories.

As described below, subsection 101(b) of the Electronic Communications Privacy Act provides an exception to the general prohibitions on interception for electronic communications which are configured to be readily accessible to the general public. Thus, the radio communications specified in proposed subsection 2510(16) are afforded privacy protections under this legislation unless another exception applies.

As specified in paragraph (A) of proposed subsection 2510(16), scrambled or encrypted radio communications are not readily accessible to the general public. The terms are used in their technical sense. To "encrypt" or to "scramble" means to convert the signal into unintelligible form by means intended to protect the contents of a communication from unintended recipients. Methods which merely change the form of a plaintext message, e.g., a device which converts an analog signal to a digital stream, does not provide "encryption" within the meaning of this bill. Nor does the use of a word code, no matter how sophisticated, amount to scrambling or encryption. Examples of scrambling techniques which are currently available include the data encryption standard (DES).

As specified in paragraph (B) radio communications transmitted through modulation techniques whose essential parameters have been withheld from the public in order to preserve the privacy of the communication are not readily accessible to the general public. This paragraph (B) refers to spread spectrum radio communications. Spread spectrum technology usually involves the transmission of a signal on different frequencies where the receiving station must possess the necessary algorythm in order to reassemble the signal.

As specified in paragraph (C) of proposed subsection 2510(16) of title 18, radio communications carried on a subcarrier or other signal subsidiary to a radio transmission are protected by the Electronic Communications Privacy Act. This category includes, for example, data and background music services carried on FM subcarriers. It also includes data carried on the Vertical Blanking Interval (VBI) of a television signal.

Radio communications transmitted over a system provided by a common carrier are not readily accessible to the general public with one exception. That exception is for tone-only paging systems. As a result of that exception, the interception of tone-only paging system transmissions will not be prohibited by this law. However, the unauthorized interception of a display paging system, which invovles the transmission of alphanumeric characters over the radio, carried by a common carrier, is illegal.

As specified in proposed paragraph (E), radio communications transmitted on frequencies allocated under parts 25 and 94 and subparts D, E, an F of part 74 of the FCC rules are protected by the Electronic Communications Privacy Act. These communications include satellite communications, auxiliary broadcast services and private microwave services, each of which routinely carries private business or personal communications. Two-way voice radio communications made on frequencies shared with services outside part 74 are expressly excluded from this category of protected communications.

The liability incurred under chapter 119 for the interception of the communications described in proposed paragraph 2510(16(E) may be limited. Section 101(b) of the Electronic Communications Privacy Act sets out exceptions from liability under this Act with respect to electronic communications and section 101(d) establishes the penalty structure for violations of this Act.

The term "electronic storage" is defined in proposed subsection 2510(17) of title 18. Electronic storage means (A) the temporary, intermediate storage of a wire or electronic communication incidental to its transmission as well as (B) the storage of such communication by an electronic communications service for backup protection. The term covers storage within the random access memory of a computer as well as storage in any other form including storage of magnetic tapes, disks or other media. Thus, for example, section 2701's prohibitions against unauthorized access to wire or electronic communications while they are in electronic storage would prohibit unauthorized access to such a communication while it is stored on magnetic tape or disk. The section 2701 prohibitions similarly would apply to information held on magnetic tape or disk pursuant to an agreement to provide remote computing services.

The last new definition in subsection 101(a)(6) of the Electronic Communications Privacy Act is the definition of an "aural transfer" in proposed subsection 2510(18). An aural transfer means any transfer containing the human voice at any point between and including the points of origin and reception. Under this definition, voice messages transferred over a paging system are protected. It is intended that computer-generated or otherwise artificial voices are not included in this definition and thus will not be part of a "wire communication." They would, however, be part of an "electronic communication."

It is important to recognize that a transaction may consist, in part, of both electronic communications and wire or oral communications as those terms are defined in section 2510 of title 18, as amended by the Electronic Communications Privacy Act. Accordingly, different aspects of the same communication might be characterized differently. For example, the transmission of data over the telephone is an electronic communication. If the parties use the line to speak to one another between data transmissions, those communications would be wire communications. At the same time, for a person overhearing one end of the telephone conversation by listening in on the oral utterances of one of the parties, those utterances are oral communications.

Although this bill does not address questions of the application of title III standards to video surveillance and only deals with the interception of closed circuit television communications to a limited extent, closed circuit television communications do provide another example of the importance of, and the interrelationship between, the definitions contained in this legislation. If a person or entity transmits a closed circuit television picture of a meeting using wires, microwaves or another method of transmission, the transmission itself would be an electronic communication. Interception of the picture at any point without either consent or a court order would be a violation of the statute. By contrast, if law enforcement officials were to install their own cameras and create their own

closed circuit television picture of a meeting, the capturing of the video images would not be an interception under the statute because there would be no interception of the contents of an electronic communication. Intercepting the audio portion of the meeting would be an interception of an oral communication, and the statute would apply to that portion.

Section 101(b)—Exceptions with respect to electronic communications

Subsection 2511(1) of title 18 of the United States Code sets out prohibitions against the interception, disclosure and use of wire or oral communications. Subsection 2511(2) specifies conduct which is not unlawful under chapter 119 of title 18.

Subsection 101(b) of the Electronic Communications Privacy Act amends Subsection 2511(2). Paragraph 101(b), consistent with other provisions of this legislation, deletes references to common carriers. It thus clarifies that any service provider who discloses the existence of an interception or surveillance or the device used to accomplish the interception or surveillance would be liable for civil damages under Section 2520 of title 18.

Paragraph 101(b)(2) of the Electronic Communications Privacy Act amends section 2511(2)(d) of title 18 by striking out "or for the purpose of committing any other injurious act". Under current Federal law it is permissible for one party to consent to the interception of a conversation unless that interception is for illegal, tortious or other injurious purposes such as blackmail. In numerous court cases the term "other injurious purposes" has been misconstrued. Most troubling of these cases have been attempts by parties to chill the exercise of first amendment rights through the use of civil remedies under this chapter. For example, in *Boddie* v. *American Broadcasting Co.,* 731 F.2d 333 (6th Cir. 1984), the plaintiff, whose conversations were recorded by a journalist, sued. Despite the consent of the reporter who was a party to the conversation, the plaintiff claimed that the recording of the conversation was illegal because it was done for an improper purpose, to embarrass her. While the appeals court decision in *Boddie* merely sent the case back for further factual development, it is clear from the facts of the case that the term "improper purpose" is overly broad and vague. The court's opinion suggests that if the network intended to cause "insult and injury" to plaintiff Boddie, she might be entitled to recover. This interpretation of the statute places a stumbling block in the path of even the most scrupulous journalist. Many news stories have been brought to light by recording a conversation with the consent of ony one of the parties involved—often the journalist himself. Many news stories are embarrassing to someone. The present wording of section 2511(2)(d) not only provides such a person with a right to bring suit, but it also makes the actions of the journalist a potential criminal offense under section 2511, even if the interception was made in the ordinary course of responsible news-gathering activities and not for the purpose of committing a criminal act or a tort. Such a threat is inconsistent with the guarantees of the first amendment. Inasmuch as chapter 119 as amended by the Electronic Communications Privacy Act continues to prohibit interceptions made for the purpose of committing either a

crime or a tort (including defamation), the public will be afforded ample portection against improper or unscrupulous interception.

Subsection 101(b)(3) of the Electronic Communications Privacy Act amends section 2511(2)(f) of title 18 to clarify that nothing in chapter 119 as amended or in proposed chapter 121 affects existing legal authority for U.S. Government foreign intelligence activities involving foreign electronic communications systems. The provision neither enhances nor diminishes existing authority for such activities; it simply preserves the status quo. It does not provide authority for the conduct of any intelligence activity.

Further the Senate expects that the practice of providing to the House and Senate Intelligence Committees proposed changes in relevant executive branch procedures and regulations governing the conduct of intelligence activities, including those involving electronic surveillance, physical searches, and the minimization of information collected concerning U.S. persons will be continued. As in the past, the Senate expects that any relevant changes in these procedures and regulations will be provided to the Senate and House Intelligence Committees prior to their taking effect.

Finally, since Congress last addressed the issue of privacy communications in a comprehensive fashion, the technologies of communication and interception have changed dramatically, and are expected to continue to do so. These factors have raised serious issues about the protection of the privacy interests of U.S. citizens, which are of great concern to the Senate and to the American people. For this reason, the Senate wishes to emphasize the obligation of the heads of intelligence agencies to continue to keep the Select Committee on Intelligence fully and currently informed of all intelligence activities pursuant to title V of the National Security Act of 1947.

Subsection 101(b)(4) of the Electronic Communications Privacy Act amends section 2511(2)(g) of title 18 of the United States Code. It sets out new exemptions from criminal liability applicable to the technologies which this legislation adds to the privacy protections of the federal wiretap law. Proposed section 2511(2)(g) provides that it shall not be unlawful under chapters 119 or 121 of title 18 for any person to engage in the conduct described in its five subparagraphs.

Under proposed section 2311(2)(g)(i), it is permissible to intercept electronic communications made through an electronic communication system configured so that the conmmunication is "readily accessible to the general public." That term is defined with respect to radio communications in proposed section 210(16) of title 18. The term "configure" is intended to establish an objective standard of design configuration for determining whether a system receives privacy protection.

Under this provision, it would not be unlawful to intercept subcarrier and UBI communications that are transmitted for the use of the general public. Such "public" communications would include the stereo subcarrier used in FM broadcasting or data carried on the VBI to provide closed-captioning of TV programming for the hearing-impaired.

Under proposed section 2511(g)(ii) it is permissible to intercept any radio communication which is transmitted (I) by any station

for the use of the general public, or that relate to ships, aircraft, vehicles or persons in distress; (II) by any government, law enforcement, civil defense, private land mobile or public safety communications system (including police and fire), that is readily accessible to the general public; (III) by a station operating on an authorized frequency within the bands allocated to amateur, citizens band or general mobile radio services; or (IV) by any marine or aeronautical communications system.

Traditionally, these radio communications have been free from prohibitions on mere interception. Amateur radio communications, including those utilizing telephone interconnect or amateur radio computer linked message systems are certainly not those to which this legislation is aimed. All amateur radio communications conducted on radio frequencies allocated to the Amateur Radio Services are exempt from this bill's prohibitions against the interception of electronic communications.

Radio services readily accesible to the general public are exempt from this act's prohibitions against interception by the generic exception contained in proposed paragraph 2511(2)(g)(i).

Proposed section 1511(2)(g)(iii) addresses conduct which is either prohibited or permitted by the Communications Act of 1934, as amended. Under clause (I) of subparagraph (iii) it is not unlawful under chapter 119 or 121 of title 18 for any person to engage in conduct prohibited by section 633 of the Communications Act of 1934 relating to cable piracy. If an individual violates the criminal prohibitions in section 633 of the Communications Act, he cannot also be charged under chapters 119 or 121 of title 18.

Clause (II) exempts from the prohibitions on interception contained in this Act conduct which is excepted from section 705(a) of the Communications Act by virtue of section 705(b) of that Act. Thus, if conduct is permitted under section 705(b) of the Communications Act, engaging in that conduct would not be a crime under chapters 119 or 121 of title 18, as amended by the Electronic Communications Privacy Act. Determination of whether conduct is permitted under section 705(b) must, of course, be the result of an examination of the statute, relevant legislative history, existing court interpretations and constructions given the statute by appropriate federal regulatory entities.

Proposed section 2511(2)(g)(iv) of title 18 exempts from the criminal prohibition contained in chapters 119 and 121 of that title, the interception of any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station, to the extent necessary to identify the source of such interference.

Finally, proposed section 2511(2)(g)(v) exempts interceptions of radio communication by other users of the same frequency when such communication is made through a system that utilizes frequencies monitored by individuals engaged in the provision or use of such a system. This exemption clarifies that it is not unlawful for users of the same frequency, who must listen to be sure a channel is clear before using it, to do so. The exception applies to users of common and non-common carrier systems, but does not apply if the communication is scrambled or encrypted.

Subsection 101(b)(4) of the Electronic Communications Privacy Act amends subsection 2511(2) of title 18 to add a new paragraph (h) to that subsection. Proposed subparagraph (i) of paragraph (h) clarifies that the use of pen registers and trap and trace devices are not regulated by chapter 119 of title 18. The use of those devices will be regulated by new chapter 206 of title 18 as amended by the Electronic Communications Privacy Act.

Subparagraph (ii) of paragraph (h) states that no violation of this chapter occurs if a provider of wire or electronic communication service records the fact that a communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication or a user of that service, from fraudulent, unlawful or abusive use of such a service. This provision permits the electronic and wire communication providers to protect themselves and their customers.

Subsection 101(c)—Technical and conforming amendments

Subsection (c) sets out technical and conforming amendments to chapter 119 of title 18. Paragraph (c)(1) adds "electronic communication" in appropriate places throughout the chapter. Paragraph (c)(2) amends the heading of the chapter. Paragraph (c)(3) amends the table of chapters to add electronic communications to the table. Paragraphs (4), (5), (6), (7), and (8) of subsection 101(c) of the Electronic Communications Privacy Act make appropriate technical amendments to delete the term "common carrier" and substitute in its place "provider of wire or electronic communication."

Section 2511(2)(a)(i), as amended, specifies that it is not unlawful for the employees of providers of wire or electronic communication services to intercept, disclose or use customer communications in the normal course of employment while engaged in any activity which is a necessary incident to the rendition of the service or to the protection of the rights or property of the provider, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality checks.

In applying the second clause only to wire communications, this provision reflects an important technical distinction between electronic communications and traditional voice telephone service. The provider of electronic communications services may have to monitor a stream of transmissions in order to properly route, terminate, and otherwise manage the individual messages they contain. These monitoring functions, which may be necessary to the provision of an electronic communication service, do not involve humans listening in on voice conversations. Accordingly, they are not prohibited. In contrast, the traditional limits on service "observing" and random "monitoring" do refer to human aural interceptions and are retained with respect to voice or "wire" communications.

Subsection 101(d)—Penalties modification

Subsection 101(d) of the Electronic Communications Privacy Act modifies the general penalty structure for violations of this chapter. It sets out proposed subsections (4) and (5) of section 2511 of title 18. Subsection (4) sets out the criminal penalties for violations

of subsection 2511(1). Subsection (5) outlines the injunctive relief available to the federal government in the case of specified conduct related to private satellite video communications that are not scrambled or encrypted and to communications transmitted on frequencies allocated under subpart D of part 74 of the FCC rules that are not scrambled or encrypted.

The general rule as set out in proposed paragraph 2511(4)(a) is that a violation is punishable as a 5-year felony. Unless one of the exceptions in proposed subsection 2511(4)(b) or subsection 2511(5) applies, a person violating section 2511(1) will be liable for a fine under this chapter, imprisonment up to 5 years, or both. The fines under the chapter are set by section 3623 of title 18. That section provides for a different maximum fine level for felonies or misdemeanors resulting in death. Individual defendants can be fined up to $250,000 and organizations can be fined up to $500,000.

As stated in proposed paragraph 2511(14)(b), the first exception to the general rule that violations are 5-year felonies, applies to unscrambled, unencrypted radio communications provided that the conduct is a first offense and is not for a tortious or illegal purpose or purposes of direct or indirect commerical advantage or private financial gain. If the radio communication is scrambled or encrypted, if the person violating the statute has been found guilty of a prior offense, or if his conduct was for one of the enumerated bad purposes, the conduct remains punishable as a 5-year felony.

As stated in subparagraph (ii) of proposed paragraph 2511(4)(b), for first offenders whose conduct was not for one of the enumerated bad purposes, if the communication is not scrambled or encrypted and it is the radio portion of a cellular telephone, public land mobile radio service or paging service communication, then the violator will be subject to a $500 criminal fine. Otherwise, as stated in clause (i) of proposed paragraph 2511(4)(b), the conduct is punishable as a one-year misdemeanor with fines of up to $100,000, 18 U.S.C. 3623, unless the conduct is that described in subsection (5).

It should be noted that the exceptions set out in proposed paragraph 2511(4)(b) apply only to radio communications. The interception of "wire" communications remain punishable as five-year felonies. The interception of the wire portion of a cellular telephone call, for example, is a five-year felony.

Proposed paragraph 2511(4)(c) decriminalizes certain conduct unless it is for the purposes of direct or indirect commercial advantage or private financial gain. The terms "direct or indirect commercial advantage or private financial gain" are intended to have the same meaning as those terms have when they are used in 47 U.S.C. 705(b).

This exception from the criminal provisions of the Electronic Communications Privacy Act applies to the interception of an unencrypted, unscrambled satellite transmission that is transmitted (i) to a broadcasting station for purposes of retransmission to the general public; or (ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls. The conduct described in subparagraphs (i) and (ii) is not an offense under this chapter and is not subject to civil liability under this chapter.

Subparagraph (i) decriminalizes the interception of "network feeds" under title 18. Such conduct will be governed exclusively by section 705 of the Communications Act (47 U.S.C. 705).

Subparagraph (ii) decriminalizes the interception of material transmitted as an audio subcarrier provided that the information is intended for redistribution to facilities open to the public. Audio subcarriers intended for redistribution to facilities open to the public include those for redistribution by broadcast stations, cable TV systems and like facilities. They also include those for redistribution to buildings open to the public, and thus, it would not be unlawful to intercept music transmitted via an audio subcarrier if it is intended for redistribution to buildings like hospitals and office buildings which pump music into their lobbies and other public areas.

Subparagraph (ii) does not apply to data transmissions or telephone calls. The interception of those transmissions, like the interception of transmissions made for the enumerated bad purposes, would be punishable as 5-year felonies.

The private viewing of satellite cable programming, network feeds and certain audio subcarriers will continue to be governed exclusively by section 705 of the Communications Act of 1934, as amended, and not by chapter 119 of title 18 of the United States Code.

A new government action for injunctive relief is set out in proposed subsection 2511(5) of title 18. This new subsection was created to underscore that this public injunctive action is distinct from the criminal penalties set out in subsection (4).

Its exceptions apply only if the communication is not scrambled or encrypted and the conduct is not for one of the enumerated bad purposes. Clause (A) refers to the private or home viewing of a private satellite video communication. With regard to the home viewing of private satellite video communications, for purposes of this provision and proposed section 2520, the Committee views as scrambling that type of multiplexing [2] in which the audio and video portions of a communication are split, requiring special equipment to reassemble the whole communication (generally a videoteleconference) before it can be received in intelligible form. Clause (B) refers to radio communications transmitted on frequencies allocated under subpart D of part 74 of the FCC rules.

Under proposed clause 2511(5)(a)(ii)(A), if the violation is a first offense and the person has not previously been found liable in a private civil action under section 2520 of title 18, the government may sue for appropriate injunctive relief. Under proposed clause (B) if the violation is a second or subsequent offense or the person has previously been found liable under section 2520, he shall be subject to a mandatory $500 civil fine.

Proposed paragraph (b) of subsection 2511(5) clarifies that the court may use any means within its existing authority, including civil or criminal contempt, to enforce an injunction issued to an individual under this subsection. Paragraph (b) also requires that the court impose a civil fine of $500 or more for each violation of such

[2] Multiplexing refers to the transmission of communications by means of modulation techniques whose essential parameters have been withheld from the public.

an injunction. The term "violation" in this context refers to each viewing of a private video communication and to each reception of a part 74 D radio communication.

Subsection 101(e)— Exclusivity of remedies with respect to electronic communications

Subsection 101(e) of the Electronic Communications Privacy Act amends subsection 2518(10) of title 18 to add a paragraph (c) which provides that with respect to the interception of electronic communications, the remedies and sanctions described in this chapter are the only judicial remedies and sanctions available for nonconstitutional violations of this chapter involving such communications. In the event that there is a violation of law of a constitutional magnitude, the court involved in a subsequent trial will apply the existing Constitutional law with respect to the exclusionary rule.

The purpose of this provision is to underscore that, as a result of discussions with the Justice Department, the Electronic Communications Privacy Act does not apply the statutory exclusionary rule contained in title III of the Omnibus Crime Control and Safe Streets Act of 1968 to the interception of electronic communications.

Similarly, the Electronic Communications Privacy Act does not amend the Communications Act of 1934. Conduct in violation of that statute, will continue to be governed by that statute.

Subsection 101(f)—State of mind

Subsection 101(f) of the Electronic Communications Privacy Act changes the state of mind required to violate section 2511 or section 2512 of title 18 of the United States Code from "willful" to "intentional." The purpose of this amendment is to underscore that inadvertent interceptions are not crimes under the Electronic Communications Privacy Act.

As used in the Electronic Communications Privacy Act, the term "intentional" is narrower than the dictionary definition of "intentional." "Intentional" means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective. An "intentional" state of mind means that one's state of mind is intentional as to one's conduct or the result of one's conduct if such conduct or result is one's conscious objective. The intentional state of mind is applicable only to conduct and results. Since one has no control over the existence of circumstances, one cannot "intend" them.

As indicated in the Judiciary Committee's report to accompany the Criminal Code Reform Act of 1981 (S. 1630):

> The highest degree of culpability is present if a person engages in conduct (or causes a result) *intentionally,* that is, "if it is his conscious objective or desire to engage in the conduct (or cause the result)." A common means to describe conduct as intentional, or to say that one causes the result intentionally, is to state that it is done or accomplished "on purpose."

> The term "intentional" is not meant to connote the existence of a motive. Liability for intentionally engaging in prohibited conduct is not dependent on an assessment of the merit of the motive that led the person to disregard the law. (Emphasis in original; citation omitted.) Report of the Committee on the Judiciary, United States Senate, to accompany S. 1630, Criminal Code Reform Act of 1981, Report 97-307 at 67.

The Committee went on to point out that people who steal because they like to or to get more money or to feed the poor, like Robin Hood, all commit the same crime. Id. The word "intentional" describes the mental attitude associated with an act that is being done on purpose. It does not suggest that the act was committed for a particular evil purpose.

At this point, it is important to note that the crime of interception under the Electronic Communications Privacy Act consists of the intentional acquisition of the contents of a wire, electronic or oral, communication through the use of any electronic, mechanical, or other device. Some groups which engage in testing were concerned that the picking up of the contents of a communication incident to those tests might be considered a crime under title III as amended by the Electronic Communications Privacy Act.

They then sought exemptions from liability under proposed paragraph 2511(2)(g). The Subcommittee on Patents, Copyrights and Trademarks rejected this approach solely because it feared application of the principle of statutory construction of "expressio unius, est exclusio alterius" would encourage courts to treat similar tests as unlawful.

For example, since the early 1960s, motor vehicle manufacturers and others have been committed to voluntary actions to make their products "good citizens" in the electromagnetic environment. That commitment has fostered the development of test procedures and programs resulting in systems to help ensure that the electromagnetic energy radiated from equipment such as motor vehicles, agricultural and construction machinery, engines for transportation, marine, industrial and consumer applications, electronic equipment and components of the foregoing do not interfere with signals carrying video, voice or data transmissions. Personal, business and entertainment radio, television, digital data communications, and radio navigation services are examples of services benefited by such test procedures and programs.

The equipment for measuring the test procedures and technical specifications by which electromagnetic radiation from motor vehicles typically includes an antenna for picking up electromagnetic energy radiated from the vehicle, and a radio receiver for scanning the frequency range from 20 or 30 to 1,000 MHz to determine the field strength of all emissions in that range which the antenna picks up.

The antenna picks up not only the electromagnetic emissions from the equipment being tested, but also any other signals present at the antenna location. Indeed, to be able to quantify the strength of the emissions to be measured, even though additional signals are present at the frequency on which the measurement is being made,

the procedures and programs specify initial measurement of these additional signals. Of course, any radio service operating in the scanned frequency range will be picked up and its field strength measured during both the baseline and the vehicle tests. Although occasionally a speaker will be used to verify that a radio service is indeed producing a high field strength reading, in virtually all of the testing there is not attempt to ascertain the substance, purport or meaning of the signal.

Similar equipment and procedures are used to measure electromagnetic radiation emitted by computing devices. In addition, the operation of electronic equipment, and devices equipped with electronic controls, may be susceptible to disruption by electromagnetic radiation impinging on such equipment or devices. For example, the operation of electronic engine controls, electronic speed controls, and anti-lock brake systems employing electronic controls, and even the operation of heart pacemakers, are potentially susceptible to disruption by strong electromagnetic radiation.

To help design equipment and devices which are resistant to such disruption, such equipment and devices customarily are irradiated during their development with electromagnetic engery at a variety of radio frequencies, and the effects, if any, of such irradiation on their operation are observed. To avoid interference with ongoing radio services, it is essential that the test engineer, before turning on the radio transmitter used for such irradiation, listen on the transmitter frequency to ascertain that there is no other signal on that frequency with which the test transmission might interfere.

In addition, both the EPA and the FCC have pointed out that Federal agencies and state and local governments are currently addressing the problem of potentially excessive public exposure to radio frequency (RF) radiation emitted by various kinds of equipment. Testing solely to determine the source of, or to measure, RF emissions in order to comply with or to establish or enforce applicable federal, state or local standards limiting human exposure to RF radiation is not prohibited by the Electronic Communications Privacy Act.

This legislation was never intended to outlaw such testing, conducted in the ordinary course of the tester's business or regulatory activities. However, if one who obtained information in the course of such a test went beyond the procedures of the test to use any information obtained through the testing process, he could violate this statute.

Section 102—Requirements for certain disclosures

Section 102 of this legislation amends section 2511 of title 18 of the United States Code to add a new criminal prohibition on disclosure of electronic communications. It adds a new subsection (3) to section 2511. This amendment includes the term "to the public." The Government is included as part of the public. Thus, FTS services are covered.

The language in paragraph (a) of proposed subsection 2511(3) of title 18 provides that a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person

or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or the agent of such addressee or intended recipient.

Proposed paragraph (b) of new subsection 2511(3) of title 18 sets out exceptions to paragraph (a)'s criminal prohibition on disclosure. Providers of electronic communication services to the public are permitted to divulge the contents of any such communication (i) as otherwise authorized in section 2511(2)(a) or 2517 or title 18; (ii) with the lawful consent of the originator or any addressee or intended recipient; (iii) to any person employed or authorized, or whose facilities are used, to forward such communication to its destination, or (iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime if such divulgence is made to a law enforcement agency.

The exceptions to the divulgence bar are relatively straightforward. Providers should be permitted to divulge under other provisions of the chapter. To be consistent with the one party consent exception found in the chapter, a similar exception is appropriate here. It is also logical to provide an exception with respect to activities necessary and intrinsic to the communication activity. Therefore, it is necessary to exempt communication intermediaries.

Finally, if an electronic communications service provider inadvertently obtains the contents of a communication during transmission and the communication appears to relate to the commission of a crime, divulgence is permitted when such divulgence is made to a law enforcement agency. If the provider purposefully sets out to monitor conversations to ascertain whether criminal activity has occurred, this exception would not apply.

Section 103—Recovery of civil damages

Section 103 of the Electronic Communications Privacy Act amends existing section 2520 of title 18 of the United States Code to incorporate violations involving interception, disclosure or intentional use of wire, oral, or electronic communications.

Proposed subsection 2520(a) of title 18 authorizes the commencement of a civil suit. There is one exception. A civil action will not lie where the requirements of section 2511(2)(a)(ii) of title 18 are met. With regard to that exception, the Committee intends that the following procedural standards will apply:

(1) The complaint must allege that a wire or electronic communications service provider (or one of its employees): (a) disclosed the existence of a wiretap; (b) acted without a facially valid court order or certification; (c) acted beyond the scope of a court order or certification or (d) acted on bad faith. Acting in bad faith would include failing to read the order or collusion. If the complaint fails to make any of these allegations, the defendant can move to dismiss the complaint for failure to state a claim upon which relief can be granted.

(2) If during the course of pretrial discovery the plaintiff's claim proves baseless, the defendant can move for summary judgment.

(3) If the court denies the summary judgment motion, the case goes to trial. At the close of the plaintiff's case, the de-

fendant again can move for dismissal. If that motion is denied, the defendant then has the opportunity to present to the jury its section 2520 good faith defense.

The plaintiff may bring a civil action under section 2520 whether or not the defendant has been subject to a criminal prosecution for the acts complained of, but in the absence of such prosecution and conviction, it is the plaintiff's burden to establish that the requirements of this section are met.

Proposed subsection 2520(b) indicates that appropriate relief in a civil action can include: (1) 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 reasonable litigation costs.

Proposed subsection 2520(c) provides a method for the computation of damages. The general rule is set out in paragraph (2) of subsection (c). The court may assess damages consisting of whichever is the greater of (A) the sum of the plaintiff's actual damages and any profits the violator made as a result of the violation; or (B) statutory damages of whichever is the greater of $100 a day or $10,000.

An exception from that general rule is set out in proposed paragraph (1) of subsection 2520(c). This exception applies if the violation consists of the private or home viewing of an unencrypted or unscrambled private satellite video communication or if the communication is an unencrypted or unscrambled radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the FCC rules, and the conduct is not for one of the enumerated bad purposes.

Under subparagraph (A), if the violator has not previously been enjoined in a government action under subsection 2511(5) and has not been found liable in a prior civil action, the court shall assess the greater of the sum of the plaintiff's actual damages or statutory damages of $50 to $500. Under subparagraph (B), if the violator is a second offender (one who has been found liable in a prior private civil action under section 2520 or one who has been enjoined in a government suit), the court shall assess the greater of the sum of the plaintiff's actual damages or statutory damages of $100 to $1000. Third and subsequent offenders are subject to the bill's full civil penalties as described in the general rule set out in proposed paragraph 2520(c)(2).

Subsection 2520(d) provides a good faith defense for those who comply with court orders or warrants, grand jury subpoenas, legislative or statutory authorizations, or a request of an investigative or law enforcement officer under section 2518(7) of title 17 concerning emergency situations. As used in this subsection, the term "good faith" includes the receipt of a facially valid court order. The fact that the provider of a wire or electronic communication service received a facially valid court order means that the provider would be entitled to a dismissal of a civil action upon a showing that he acted within the scope of that order.

Proposed subsection 2520(e) sets out the statute of limitations for actions brought under this section. Actions may not be commenced more than 2 years after the date on which the claimant first has a reasonable opportunity to discover the violation.

Section 104—Certain approvals by justice department officials

Section 104 of the Electronic Communications Privacy Act amends section 2516(1) of title 18 of the United States Code to add to the list of Federal officials who may make applications for court orders under chapter 119. Under this amendment, the list of officials who may be specially designated by the Attorney General to authorize applications will include any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division. The addition of an acting Assistant Attorney General is not meant to imply rejection in any other context of the well-established principle that an acting official ordinarily possesses all the legal powers of the official for whom he is acting, but to clarify the law under this statute.

As indicated in proposed subsection 111(c) of the Electronic Communications Privacy Act, this section 104 shall take effect on the date of enactment.

Section 105—Addition of offenses to crimes for which interception is authorized

Section 105 of the Electronic Communications Privacy Act amends existing section 2516 of title 18 to add to the list of felonies for which a wiretap or bugging order may be obtained under chapter 119. It also adds a new subsection (3) to section 2516 which addresses applications and orders for interceptions of electronic communications.

Subsection 105(a)—Offenses for which wire and oral interceptions are authorized

Subsection 105(a) of the legislation amends subsection 2516(1) of title 18 by adding to the list of predicate felonies for which an application for a wiretapping or bugging order may be made. Those crimes are set out in the bill.

Subsection 105(b)—Offenses for which interception of electronic communication are authorized

Subsection 105(b) of the Electronic Communications Privacy Act amends section 2516 to authorize the Government to apply for a court order authorizing or approving the interception of an electronic communication by an investigative or law enforcement officer when an interception may provide or has provided evidence of a Federal felony. Thus, for non-wire, non-oral electronic communications, a different and less restrictive list of crimes can be used to justify an application for interception.

The Department of Justice has advised the Committee on the Judiciary that for the three years which follow the date of enactment of this legislation, this authority will only be exercised pursuant to the approval of the same level of officials as those involved in the approval of applications for wire interceptions. In addition to this voluntary regulatory limitation, the Department of Justice has committed itself to submitting to the relevant congressional committees any proposed changes in these regulations at least 90 days in advance of any change.

Section 106—Applications, orders, and implementation of orders

Section 106 of the Electronic Communications Privacy Act amends section 2518 of title 18 of the United States Code. This section addresses the implementation of interception orders, reimbursement for providers who assist law enforcement agencies in carrying out an interception order and minimization requirements. Subsection 106(d) of the legislation permits law enforcement agencies to request an order for a "roving tap" under certain limited circumstances.

Telephone companies have, as a matter of practice, provided information and technical assistance to law enforcement officials in connection with lawfully authorized wiretaps. They have steadfastly maintained, however, an important distinction between such technical assistance and any active participation in the wiretap itself.

Section 2518(4) of title 18 is a codification of the cooperative working relationship that exists between telephone companies and law enforcement officials. This section anticipates that these government officials will, and should, seek the cooperation of telephone companies in accomplishing telephone line interceptions.

Nevertheless, telephone company customers have a reasonable expectation, traditionally enhanced by telephone company practices and policies, that their company will not become in effect, a branch of Government law enforcement. Accordingly, while technical assistance is provided and paid for, the Committee wishes to make clear that Section 2518(4) is not intended to authorize and should not be construed as authorizing, issuance of an order for land line telephone company assistance which either requires a company to actually accomplish or perform a wiretap or requires that law enforcement wiretap activity take place on land line telephone company premises.

The Committee understands that some cellular service providers may have cooperated with law enforcement officials to establish wiretap connections on the cellular service provider's premises. The Committee does not intend to alter this specific form of assistance.

The Committee understands that the practice followed with regard to land line telephones is that telephone company employees do not perform the wiretap itself, and that telephone company premises are not used for wiretap activity. This procedure is accepted by both company and law enforcement officials. The Committee does not expect any departure from current practice.

To ensure that the practice does not change, absent a compelling need appropriately addressed to Congress, the Committee expects the Justice Department to include in its United States Attorneys Manual a statement that no enforcement agency or official shall attempt to compel any telephone company employee to perform any wiretap, or attempt to compel any such company to make its premises available for wiretap activity. Any proposed amendment to that language should be reported to the Committee well in advance of dissemination so that the Committee has sufficient opportunity to assess both the extent of which such proposed language comports with its view of the scope of section 2518(4) as expressed

above and the extent to which any amendment of section 2518(4) to permit a change in prevailing practice may be warranted by subsequent and compelling changes in technology or other circumstances.

Subsection 106(a)—Place of authorized interception

Subsection 106(a) of the Electronic Communications Privacy Act amends subsection 2518(3) of title 18. It provides, that in the case of a mobile interception device, a court can authorize an order within its jurisdiction and outside its jurisdiction but within the United States. This provision applies to both a listening device installed in a vehicle and to a tap placed on a cellular or other telephone instrument installed in a vehicle.

In most cases, courts will authorize the installation of a device and the device will be installed within the court's jurisdiction, but the suspect will subsequently move outside that jurisdiction. In certain cases, however, a device authorized for installation in an automobile may be authorized in one district and the vehicle might be moved to another district prior to installation. Subsection 106(a) of the bill permits installation in the district to which the vehicle has been moved.

Nothing in this subsection affects the current law with regard to the use of such devices outside the United States.

Subsection 106(b)—Reimbursement

Subsection 106(b) of the Electronic Communications Privacy Act establishes that service providers that provide assistance to the agency carrying out an interception order may be compensated for reasonable expenses incurred in providing such facilities or assistance. This is designed to permit reimbursement at an amount appropriate to the work required. In most cases, a flat or general rate will be appropriate, but this change in the existing law will permit flexibility by authorizing reimbursement at a higher level in unusual cases.

Subsection 106(c)—Minimization

This subsection makes two changes in section 2518(5) of title 18. Under existing law, no section 2518 interception order may extend longer than 30 days. Paragraph (1) of subsection 106(c) provides a rule for establishing when the 30 days to install a tap or a bug begins to run. Under this rule, the 30-day time period commences on the earlier of the day on which the officer first begins to conduct the interception, or 10 days after the order is entered.

Paragraph (2) of this subsection of the Electronic Communications Privacy Act provides a special minimization rule for intercepted communications that are in code or in a foreign language. If an expert in that foreign language or code is not reasonably available during that interception period, minimization may be accomplished as soon as practicable after the interception. In this regard, it is contemplated that the translator or decoder will listen to the tapes of an interception and make available to the investigators the minimized portions preserving the rest for possible court perusal later.

Paragraph (2) also provides that the monitoring of interceptions under this chapter may be conducted in whole or in part by Government personnel, or by individuals operating under contract with the Government, as long as such personnel are acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception. This change, which was sought by the Federal Bureau of Investigation, is designed to free field agents from the relatively routine activity of monitoring interceptions so that they can engage in other law enforcement activities.

The Committee recognizes that although the statutory standards for minimizing wire, oral, and electronic communications are the same under proposed subsection 2518(5), the technology used to either transmit or intercept an electronic message such as electronic mail or a computer data transmission ordinarily will not make it possible to shut down the interception and taping or recording equipment simultaneously in order to minimize in the same manner as with a wire interception. It is impossible to "listen" to a computer and determine when to stop listening and minimize as it is possible to do in listening to a telephone conversation. For instance, a page displayed on a screen during a computer transmission might have five paragraphs of which the second and third are relevant to the investigation and the others are not. The printing technology is such that the whole page including the irrelevant paragraphs, would have to be printed and read, before anything can be done about minimization.

Thus, minimization for computer transmissions would require a somewhat different procedure than that used to minimize a telephone call. Common sense would dictate, and it is the Committee's intention, that the minimization should be conducted by the initial law enforcement officials who review the transcript. Those officials would delete all non-relevant materials and disseminate to other officials only that information which is relevant to the investigation.

Subsection 106(d)—Roving taps

This subsection of the Electronic Communications Privacy Act adds a new subsection (11) to section 2518 of title 18. Under current law, the application and the order for a bug or tap must indicate the "particular" facility or place in which the interception is to occur. Subsection 106(d) of this legislation sets out new rules for the specificity required in the description of the place where the interceptions of wire and oral communications are to occur. The Committee finds such a provision necessary to cover circumstances under which law enforcement officials may not know, until shortly before the communication, which telephone line will be used by the person under surveillance. Telephone companies assist law enforcement officials by providing cable and pair information, or leased line facilities when requested and feasible: this is the information which will be provided to law enforcement for roving taps.

In the case of both oral and wire communications, only a limited list of Federal officials can apply for a special order seeking relief under this provision.

With regard to "oral" communications, as set out in paragraph (a) of proposed subsection 2518(11), an application for a special

order must contain a full and complete statement as to why the ordinary specification requirements are not practical. The application must also identify the person committing the offense and whose communications are to be intercepted. The judge must find that the ordinary specification rules are not practical. Situations where ordinary specification rules would not be practical would include those where a suspect moves from room to room in a hotel to avoid a bug or where a suspect sets up a meeting with another suspect on a beach or a field. In such situations, the order would indicate authority to follow the suspect and engage in the interception once the targeted conversation occurs.

The rule with respect to "wire communications" is somewhat similar. As indicated in paragraph (b), the application must show that the person committing the offense has a purpose to thwart interception by changing facilities. In these cases, the court must find that the applicant has shown that such a purpose has been evidenced by the suspect. An example of a situation which would meet this test would be an alleged terrorist who went from phone booth to phone booth numerous times to avoid interception. A person whose telephone calls were intercepted who said that he or she was planning on moving from phone to phone or to pay phones to avoid detection also would have demonstrated that purpose.

Proposed subsection 2518(12) of title 18 provides, with respect to both "wire" and "oral" communications, that where the federal government has been successful in obtaining a relaxed specificity order, it cannot begin the interception until the facilities or place from which the communication is to be intercepted is ascertained by the person implementing the interception order. In other words, the actual interception could not begin until the suspect begins or evidences an intention to begin a conversation.

It would be improper to use this expanded specificity order to tap a series of telephones, intercept all conversations over such phones and then minimize the conversations collected as a result. This provision puts the burden on the investigation agency to ascertain when the interception is to take place.

The Subcommittee on Patents, Copyrights and Trademarks added a provision to proposed subsection 2518(12) allowing a service provider to move the court to modify or quash the order on the grounds that it cannot provide assistance in a timely or reasonable manner. As indicated, on notice to the Government, the court must decide such a motion expeditiously.

This provision recognizes that a telephone company may not be able to respond instantaneously to an eleventh hour target line designation. It is designed to account for the practicalities of telephone company response time, the number of phones that may be covered by the order, and the geographic area of the target lines that may be used by the person under surveillance.

The Committee intends that the court look to several factors in considering whether to issue an order pursuant to proposed paragraph (11)(b). The request for the order, and the order itself, should specify a reasonably limited geographic area, the number of phones (and phone numbers) if known, to be intercepted—so as not to render telephone company cooperation technically infeasible—and the time within which the interception is to be accomplished. The

failure to make such specifications in the request and/or in the order may be considered evidence of unreasonableness or untimeliness by a court acting upon a telephone company motion made pursuant to proposed subsection (12).

The Committee also expects law enforcement officials to continue the current practice of consulting with telephone company employees regarding the details of implementation (such as phone numbers and the specific locations of the telephones) in advance of the time any order for interception is sought.

Finally, subsection 106(d) of the Electronic Communications Privacy Act provides that reports to the Administrative Office of the United States Courts under current section 2519 of title 18 on the kind of order or extension applied for include whether or not the order was one applied for under the relaxed specifity provisions of subsection 2518(11).

Section 107—Intelligence activities

Subsection (a) of this section of the bill clarifies that the amendments made in subsection 102(b) of the bill do not provide any new authority for intelligence activities but only represent an exemption from the coverage of this chapter and chapter 121 of title 18 for activities that are otherwise lawful.

Subsection (b) of this section of the bill exempts communications security monitoring activities of the Federal Government otherwise in accordance with U.S. law and undertaken in accordance with procedures approved by the Attorney General from coverage under chapter 119 or 121 of title 18. This subsection provides no new authority for such activities.

Specifically this subsection exempts from the coverage of this act the lawful activities of Federal agencies intended to intercept encrypted or other official communications for communications security purposes. Communications security measures are protective measures taken to deny unauthorized persons information derived from U.S. Government telecommunications and to ensure the authenticity of such communications. Communications security protection is the application of security measures to electrical systems generating, handling, processing, or using information the loss of which could adversely affect the national interest. Monitoring of security measures and security protection includes the intentional interception of executive branch official communications, including the communications of certain Government contractors, to provide technical material for analysis to determine the degree of security being provided to these transmissions. In addition, the interception, by authorized Federal agencies, of radio communications between foreign powers or agents as defined by the Foreign Intelligence Surveillance Act of 1978, and the accessing of electronic communications systems used exclusively by a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978, are exempted from coverage of this act by this subsection of the bill.

Section 108—Mobile tracking devices

Subsection (a) of this section of the bill adds a new section to chapter 205 of title 18. This new code section provides that if a court is empowered to issue a warrant or other order for the instal-

lation of a mobile tracking device, and the tracking of the object or person on which the device is installed, such warrant remains valid even if the device is moved outside the jurisdiction of the court, even outside the jurisdiction of the United States, provided that the device was installed within the jurisdiction of the court, in conformity with the court order. This clarification does not effect current legal standards for the issuance of such an order.

A tracking device is defined as an electronic or mechanical device which permits the tracking of the movement of a person or object.

Subsection (b) adds a new section 3117, "Mobile tracking devices" to the table of contents of chapter 205.

Section 109—Warning subject of surveillance

The section amends section 2232 of title 18 by adding at the end a new subsection. Proposed subsection 2232(c) adds two new offenses to title 18. First, it makes it a criminal act punishable by a fine under this title and/or imprisonment for not more than 5 years to warn any person that a Federal agency or law enforcement officer has been authorized or has sought authorization under chapter 119 of title 18 to intercept a wire, oral, or electronic communication. Second, the proposed subsection provides the same penalties for warning anyone that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the provisions of the Foreign Intelligence Surveillance Act.

The elements of both new crimes are the same. It is required that the defendent have knowledge that the Federal law enforcement or investigative officer has been authorized or has applied for an interception order. The defendent need not know that such an application was made under a particular chapter of federal law, rather, only that such application or order was made under federal law. The defendent must engage in conduct of giving notice of the possible interception to any person who was or is the target of the interception. Finally, the defendents action must have been undertaken with the specific intent to obstruct, impede or prevent the interception. The offense also includes an attempt to engage in the offense.

Section 110—Injunctive remedy

This section of the act sets out a proposed section 2521 of title 18. Section 2521 adds to the existing criminal and civil remedies available for violations of this chapter by authorizing the Attorney General to seek an injunction to prevent felony level violations of this chapter. Section 2521 also provides that preliminary relief can be granted to prevent a continuing and substantial injury to the United States or to any person for whose protection the action is brought. Actions under section 2521 are governed by the Federal Rules of Civil Procedure, except that when an indication has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

Section 111—Effective date

Subsection (a) provides that in general the amendments made by this act are effective 90 days after enactment, and that the act applies only with respect to court orders or extensions made after the effective date. Thus existing court orders would not be affected by these changes and on-going investigations would not be hindered, but any extention of an existing court order made 90 days after passage would be governed by these new provision.

Subsection (b) provides a special rule for the effective date in the case of state authorizations of interceptions. This special effective date rule is necessary because the provisions of chapter 119 of title 18 supersede state laws with respect to electronic communications. Under chapter 119, the states must enact statutes which are at least as restrictive as the provisions of chapter 119 before they can authorize their state courts to issue interception orders. Because of the substantial changes made by this act it is appropriate to grant the states sufficient time to modify their laws. This special effective date rule gives the states two years to amend their laws to meet the new requirements of chapter 119.

Subsection (c) provides that section 104 of the act is effective upon enactment. Section 104 modifies Justice Department procedures for approval of requests under this chapter, since section 104 is designed to alleviate management difficulties at the Department of Justice there is no reason to delay implementation of these changes.

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

Section 201—Title 18 amendment

This section amends title 18 by adding at the end thereof a new chapter 121 consisting of ten new sections. These sections are discussed below.

New section 2701—Unlawful access to stored communications

Subsection (a) of this new section creates a criminal offense for either intentionally accessing, without authorization, a facility through which an electronic communication service is provided, or for intentionally exceeding the authorization for accessing that facility. Subsection 2701, also provides that the offender must obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such an electronic storage system in order to commit a violation under the subsection. The term "electronic storage" is defined in section 2510(17) of title 18 and includes both temporary, intermediate storage of a wire or electronic communication incidental to the transmission of the message, and any storage of such a communication by the electronic communication service for purposes of backup protection of the communication.

This provision addresses the growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public.

This subsection does not prevent broad authorizations to the general public to access such a facility. The bill does not for example hinder the development or use of "electronic bulletin boards" or other similar services where the availability of information about the service, and the readily accessible nature of the service are widely known and the service does not require any special access code or warning to indicate that the information is private. To access a communication in such a public system is not a violation of the Act, since the general public has been "authorized" to do so by the facility provider.

However, the offense of intentionally exceeding an authorization to access a computer facility would apply both to public and private aspects of a system. For example, a computer mail facility authorizes a subscriber to access information in their portion of the facilities storage. Accessing the storage of other subscribers without specific authorization to do so would be a violation of this provision. Similarly, a member of the general public authorized to access the public portion of a computer facility would violate this section by intentionally exceeding that authorization and accessing the private portions of the facility.

Subsection (b) of this new section provides punishment for violation of subsection (a). A distinction is drawn between offenses committed for purposes of commercial advantage, malicious destruction or damage, or for private commercial gain and all other types of violation. If the offense is committed for private or commercial gain or for malicious destruction the subsection provides a fine of not more than $250,000 or imprisonment for not more than one year, or both, for a first offender. Second and subsequent offenders are subject to the same fine provision but a jail term up to two years can be imposed for such violations. In all other cases the fine is limited to not more than $5,000 and imprisonment for not more than 6 months or both.

Subsection (c) of this new section provides exceptions to the violations contained in subsection (a). It is not a violation of subsection (a) if the conduct was authorized by the person or entity providing the wire or communications service, or if the conduct was authorized by the user of that service with respect to communications of or intended for that user or if the conduct is authorized by new sections 2703, 2704, or 2518 or title 18.

New section 2702—Disclosure of contents

Proposed section 2702 is divided between electronic communication services and remote computing services. The restrictions on the service provider are the same in each instance. However, as described below, there is different treatment for electronic communication service providers and remote computing services with regard to government access.

Subsection (a) of this new section prohibits the provider of an electronic communications service or the provider of a remote computing service from knowingly divulging the contents of any communication. The "contents" of a communication has the same meaning in this section as it has in subsection 2510(8) of title 18 or the United States Code as amended by section 101(a)(5) of this Act. The requirement that a violator must "knowingly" divulge the con-

tents is intended to make clear that "reckless" or "negligent" conduct is not sufficient to constitute a violation of this section. Subsection (b) of this section provides exceptions to this general rule of non-disclosure.

The application of new code section 2702(a) generally prohibits the provider of a wire or electronic communication service to the public from knowingly divulging the contents of any communication while in electronic storage by that service to any person other than the addressee or intended recipient. Similarly, section 2511(3) of title 18, as amended by this Act, prohibits such a provider from divulging the contents of a communication while it is in transmission. Neither provision, however, nor any other provision in the Act, is intended to affect any other provision of federal law that prohibits the disclosure of information on the basis of the content of the information, such as the Fair Credit Reporting Act.

The application of sections 2701(a) and 2511(3) is limited to providers of wire or electronic communications services. There are instances, however, in which a person or entity both acts as a provider of such services and also offers other services to the public. In some such situations, the bill may allow disclosure while another federal requirement, applicable to the person or entity in another of its roles, prohibits disclosure. The Committee intends that such instances be analyzed as though the communication services and the other services were provided by distinct entities. Where a combined entity in its non-provider role would not be allowed to disclose, the appropriate outcome would be non-disclosure.

Subsection (b) of this new section provides exceptions to the general rule of nondisclosure provided in subsection (a). These exceptions permit disclosure: (1) to the addressee or intended recipient of the communication or the authorized agent of such addressee or intended recipient; (2) in conformity with a court order issued pursuant to the procedures in section 2516 of title 18; or in the course of normal business practice as defined in section 2511(2)(a) of this title; or to the government under procedures of new section 2703; (3) with the lawful consent of the sender or the addressee or an intended recipient of such communication or with the consent of the subscriber in the case of a remote computing service; (4) to a person employed or authorized or whose facilities are used to forward the communication to its ultimate destination; (5) as necessary in order to render the service or to protect the rights or property of the provider of the service: of (6) to a law enforcement agency, if the contents were inadvertently obtained by the service provider and appear to pertain to the commission of a crime.

The exceptions to the general rule of nondisclosure provided in subsection (b) fall into three categories. The first category are those disclosures which are authorized by either the sender or receiver of the message. Either the sender or the receiver can directly or through authorized agents authorize further disclosures of the contents of their electronic communication. The second category are disclosures which are necessary for the efficient operation of the communications system. Such business procedures are included in the section 2511(2)(a) exemption as well the exemptions of this subsection relating to the diclosure of the message to forwarding facilities and the exemption for service provider activities designed to

protect the system and perform the service. The third category are disclosures to the government. In this area there are two types of disclosures. Those pursuant to a court order under the procedures of sections 2516 and 2703 and those disclosures undertaken at the initiative of the service provider in the exceptional circumstances when the provider has become aware of the contents of a message that relate to ongoing criminal activity.

New section 2703.—Requirements for governmental access

Subsection (a) of section 2703 provides requirements for the government to obtain the contents of an electronic communication that has been in electronic storage for 180 days or less. A government entity can only gain access to the contents of such an electronic communication pursuant to a warrant issued under the Federal Rules of Criminal Procedure or an equivalent State warrant.

Subsection (b) of section 2703 provides that for electronic communications that are maintained by a remote computing service and that have been in storage in an electronic communication service for more than 180 days the Government can gain access in several ways. If the Government wishes to obtain the contents of a communication without the required notice to the subscriber then the governmental entity must obtain a warrant issued under the Federal Rules of Criminal Procedure or an equivalent State warrant. With prior notice from the government entity to the subscriber or customer, the entity may obtain the contents of the electronic communication either by using an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena or obtain a court order pursuant to subsection (d) of this section. In addition, the required notice may be delayed pursuant to the requirements of section 2705 of title 18 as provided in the Act.

Subsection (b) of new section 2703 of title 18 is made applicable to all electronic communications held or maintained by the service provider on behalf of a customer or subscriber and received by means of electronic transmission as well as electronic communications in storage or computer processing if the provider is not authorized to access the contents of any communications for purposes other than storage or computer processing.

Subsection (c) provides for access to records or other information pertaining to a subscriber to or customer of an electronic communications or remote computer service, not including the content of electronic communications. This section permits the provider of the service to divulge, in the normal course of business, such information as customer lists and payments to anyone except a Government agency. It should be noted that the information involved is information about the customer's use of the service not the content of the customer's communications.

A provider of electronic communication service or remote computing service must disclose information pertaining to a subscriber or customer, but not the contents of any communications of that customer, to a Government entity only when the Government entity either (i) uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury subpoena; (ii) obtains a warrant issued under the Federal Rules of Criminal Procedure or an equivalent state warrant; (iii) obtains a court

order for such disclosure under subsection (d) of this section; or (iv) has obtained the consent of the subscriber. A Government entity which receives customer records pursuant to one of these four alternatives is not required to provide notice to the subscriber or customer that it has requested or obtained this information.

Subsection (d) provides that orders requiring access by a Government entity to the contents of a wire or electronic communication or to the records or other information sought shall issue only if the governmental entity shows there is reason to believe the contents of the wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. This section provides no authority for the issuance of a state subpoena that is prohibited under the law of such state.

This subsection also permits the provider of the communications or remote computing service to move to quash or modify any other issued under this section if the information or records requested are unusually voluminous or compliance with the order would cause an undue burden on the provider. This specific standing for the service provider to contest an overly broad order is intended to protect the service provider from unduly burdensome requirements and to permit an impartial judicial officer to evaluate the appropriateness of the government's request.

Subsection (e)—No cause of action against a provider disclosing information under this chapter.

This subsection of the proposed new section provides a defense for the service provider, its employees and officers, from suits arising because of its disclosure of information pursuant to a warrant or other court order issued under this chapter.

New section 2704—Backup preservation

Subsection (a) of proposed section 2704 of title 18 provides that a Government entity may include in its subpoena or court order obtained pursuant to the provisions of new section 2703(b)(2) a requirement that the service provider create and maintain a duplicate copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the customer or subscriber, the service provider must create such a duplicate copy as soon as practicable and confirm to the Government entity that the duplicate file has been created. In all cases the service provider must create such a duplicate file within two business days after receipt by that provider of the subpoena or court order directing that such a duplicate file be created.

Paragraph (2) of this new subsection requires the Government entity to give notice to the subscriber or customer that such a duplicate file has been created and has been ordered to be provided to the Government. This notification to the customer or subscriber must be given within three days of the receipt of confirmation from the service provider (as required by subsection (a) above) that the duplicate file has been created, unless the Government agency has obtained permission to delay such notification pursuant to proposed subsection 2705(a).

Paragraph (3) also prohibits the service provider from destroying the backup copy until the information has been delivered to the Government entity or any proceedings, including all appeals, con-

cerning the Government's subpoena or court order have been resolved, whichever is later. The service provider is required to comply with the order and release the copy to the requesting Government entity no sooner than fourteen days after the Government entity has notified the subscriber or customer that it is seeking this information.

Paragraph (4) provides that the service provider should release the information to the Government only if the service provider has not received notice from its subscriber or customer that the subscriber or customer has challenged the Government's request and if the service provider has not itself challenged the request of the Government entity.

Finally, paragraph (5) provides that when a Government entity seeks to require the creation of the backup or duplicate copy under this subsection and the governmental entity further determines that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with the evidence this later determination is not subject to challenge either by the subscriber or customer or by the service provider.

While this subtitle provides the subscriber or customer, and in some circumstances the service provider a right to challenge the necessity for or scope of a court order, neither this section or any other section of this Act provides grounds to challenge the determination of the Government agency that no notification is to be given to the subscriber or customer of the mere creation of the duplicate file. The file is created and maintained by the service provider solely for the purpose of assuring that potential evidence is not tampered with or destroyed. Keeping the fact of the creation of this file secret does not harm any privacy interest since there are adequate safeguards included in the bill and in this chapter to control the actual release of the duplicate file to the Government agency.

Subsection (b) of proposed section 2704 provides a procedure for challenges to a court order by the subscriber or customer. The subscriber or customer whose records are sought can within 14 days after notification by the Government under subsection (a)(2) of this section file a motion to quash such subpoena or vacate such court order in an appropriate State or Federal court. The subscriber or customer challenging the subpoena or order must serve a copy of the motion on the governmental entity and provide written notice to the service provider that such a challenge has been initiated.

The subsection further provides that the application or motion must state that the applicant is the customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought and state the reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or state that there has not been substantial compliance with the provisions of this chapter in some other respect.

The service required by this subsection shall be made upon the governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, or office, or department specified in the notice which the customer has received pursuant to this chapter. The term "delivery" in this subsection has

the meaning given that term in the Federal Rules of Civil Procedure.

If a court determines that the customer or subscriber has complied with the requirements for such a motion including the requirements of "delivery" to the Government entity, then the court shall order the Government entity to file a sworn response to the motion or application. Such response may be in camera if the governmental entity includes in its response the reasons which make such an in camera review appropriate. If the motion and response provide insufficient information for the court to make a determination, the court may conduct such additional proceedings as it deems appropriate. Any additional proceedings and a decision on the challenge shall occur as rapidly as feasible, *i.e.* within 7 calendar days in all but the most unusual circumstances.

The subsection also provides that the court shall enforce the process if it finds that the applicant challenging the order or application is not the subscriber or customer for whom the records are maintained or if it finds that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry. If the court finds that the customer or subscriber challenging the order or application is the subscriber or customer for whom the records are maintained and that the records are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect, then the court shall order the process quashed.

Finally, the subsection provides that a court order denying a motion or application under section 2704 shall not be deemed a final order and no interlocutory appeal may be taken by the customer or subscriber from such a denial.

In the event that there is no indictment then the person whose records are involved may move for the return of the records. Obviously, nothing precludes a customer or subscriber who is later the subject of a criminal proceeding from raising these issues again subject to the sanctions limitation of section 2708 of title 18.

New section 2705—Delayed notice

This proposed section provides procedures and requirements for implementation for a delay of notice to the customer or subscriber that his records are being sought or have been provided to a government entity.

Subsection (a) of this section 2705 provides that when a Government entity seeks or obtains access to the contents of an electronic communication by application for a court order notification can be delayed for an initial period of up to 90 days, if the Government entity requests such a delay and the court determines that there is reason to believe that the notification of the existence of the court order may have an adverse result as described in this subsection. Where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, a delay of notification for a period of not more than 90 days can be obtained upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result.

For purposes of a delay of notification, an adverse result is defined as (A) endangering the life or physical safety of an individual; (B) flight from prosection; (C) destruction of or tampering with evidence; (D) intimidating of potential witnesses; or (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

In the case of an administrative or grand jury subpoena, the governmental entity is required to maintain a true copy of the required certification, and the certification can only be given by a "supervisory official". The subsection defines such an official as the investigative agent in charge of an agency's headquarters or regional office, or the assistant to such an agent or the equivalent, or the chief prosecuting attorney or the first assistant prosecuting attorney of an agency's headquarters or regional office, or the equivalent.

The subsection also provides that extensions of the delay period for not more than 90 days each may be granted by the court upon application or by certification by the government agency provided the requirements of subsection (b) of section 2705 are met for each extension.

When the delay period, including any extensions thereof, as provided in this subsection and subsection (b), has expired the governmental entity must serve upon, or deliver by registered or first-class mail to the customer or subscriber, a copy of the process or request together with notice that states the nature of the law enforcement inquiry and informs the customer or subscriber: (i) that the information maintained for such customer or subscriber by the service provider was supplied or requested by the Government agency and stating the date on which the information was supplied or requested; (ii) that notification to the customer of this action was delayed; (iii) what Government entity or court made the certification or determination that notification could be delayed; and (iv) which provision or provisions of this chapter allowed the delay.

Subsection (b) provides that if a governmental entity has delayed notice or has not been required to give notice under the provisions of section 2703, then the governmental entity may also apply to the 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, not to notify any person of the existence of the warrant, subpoena, or court order. The court is required to enter such an order to prevent disclosure by the service provider if notification of the existence of the warrant, subpoena, or court order will result in any of the five adverse results listed in this subsection. The entity must apply to a court for preclusion under this subsection, even if the underlying process—an administrative subpoena, for example—does not require a court order.

New section 2706—Cost reimbursement

This proposed section provides that when a governmental entity obtains the contents of communications, records or other information under the authority of sections 2702, 2703, or 2704, it shall pay to the person or entity assembling or providing the information a fee for reimbursement for the reasonably necessary direct costs. The section provides an exception to this general rule with regard to records or other information maintained by a communications

common carrier that relate to telephone toll records and telephone listings obtained under section 2703. No fee is normally required for access to such records. However, the court may order a payment if the court determines the information required is unusually voluminous. The amount of the fee provided in this subsection is to be mutually agreed upon by the governmental entity and the person or entity providing the information. If they are unable to reach an agreement, the court which issued the order for production of the information, or the court before which a criminal prosecution relating to the information would be brought if no court order was issued, is empowered to determine a reasonable fee.

New section 2707—Civil action

Subsection (a) of this proposed section provides that, except as provided in section 2703(e), any provider of electronic communication service, subscriber, or customer of such service aggrieved by any violation of this new chapter may recover from any person or entity—including governmental entities—who knowingly or intentionally violated this chapter.

Under subsection (b), appropriate relief in a civil action under this title includes: (1) such preliminary, declaratory, or other equitable relief as may be appropriate; (2) damages under the section including the sum of actual damages suffered by the plaintiff and any profits made by the violator as the result of the violation as provided in (c) with minimum statutory damages of $1,000; and (3) reasonable attorney's fees and other reasonable litigation costs.

The section also provides a defense to an action under this chapter. If the defendant's action was based on a good faith reliance on a court order or warrant, a grand jury subpoena, a legislative or statutory authorization; or a request of an investigative or law enforcement officer under section 2518(7) of this title, or if it was based on a good faith determination that section 1511(3) of this title permitted the conduct complained of, then this good faith reliance or determination is a complete defense to any civil or criminal action brought under this chapter or under any other law.

This new section also provides that any action under this section must be commenced not later than 2 years after the date upon which the claimant first discovered or had a reasonable opportunity to discover that a violation had occurred.

New section 2708—Exclusivity of remedies

The remedies and sanctions provided in this chapter are the only judicially available remedies and sanctions for nonconstitutional violations of the chapter.

New section 2709.—Counterintelligence access to telephone toll and transactional records

Section 2709 provides for FBI counterintelligence access to telephone toll and transactional records. This provision is substantially the same as language recently reported by the Intelligence Committee as section 503 of the Intelligence Authorization Act for Fiscal Year 1987. There are two differences. The first is that section 2709 applies not only to FBI requests for telephone subscriber information and toll billing information, but also to FBI requests

for electronic communication transactional records. This ensures that the FBI has the necessary authority with regard to subscriber information and toll billing information with respect to electronic communication services other than ordinary telephone service.

Section 2709 is a carefully balanced provision that remedies the defect in current law that the FBI cannot gain access on a mandatory basis to telephone toll records maintained by communications common carriers, for counterintelligence purposes. As a result, especially in states where public regulatory bodies have created obstacles to providing such access, the FBI has been prevented from obtaining these records, which are highly important to the successful investigation of counterintelligence cases.

The second difference concerns the standard that the FBI must meet before it can require a common carrier or service provider to supply the requested records. Section 2709 requires a certification by a designated FBI official that the information sought is relevant to an authorized foreign counterintelligence investigation and that there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978. Section 503 of the Intelligence Authorization Act for Fiscal Year 1987, as reported by the Intelligence Committee, contains a slightly different "reason to believe" standard requiring specific and articulable facts giving reason to believe that the target "is or may be" a foreign power or an agent of a foreign power.

Subsection 2709(a) of this proposed section provides that a wire or electronic communication service provider must comply with a request for subscriber information and toll billing records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section. It should be noted that this applies only to transactional records, not to the content of the electronic messages of a customer or subscriber.

Subsection 2709(b) provides that in order for the requirement to provide information in subsection (a) of this section to apply, the Director of the Federal Bureau of Investigation, or a specific person within the Bureau designated for this purpose by the Director, must certify in writing to the wire or electronic communication service provider that (1) the information sought is relevant to an authorized foreign counterintelligence investigation; and (2) that there are specific, articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act.

The House Judiciary Committee report on the Electronic Communications Privacy Act of 1986 does not discuss the meaning of the "reason to believe" standard in section 2709. It is essential, therefore, to clarify the intent of the Senate with respect to this item.

The "reason to believe" requirement in section 2709 is intended to be substantially less stringent than the requirement of "probable cause." It is intended that the application of the "reason to believe" requirement will be determined by a senior FBI official at the level of Deputy Assistant Director or above. It is intended that

in applying the "reason to believe" standard to a specific case, the FBI official may take into account any facts or circumstances that a prudent investigator would consider, so long as there is an objective, factual basis of the determination.

The Senate Select Committee on Intelligence has informed the Judiciary Committee that the language contained in the bill would not significantly affect the application of the current FBI investigative standard in this area. Further discussion of the investigatory standard in particular cases is contained in the reports of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence on FY 87 Intelligence Authorization Act (S. 2477 and H.R. 4759).

Subsection 2709(c) prohibits a service provider, or any officer, employee, or agent of the service provider from disclosing to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

Subsection 2709(d) permits the Federal Bureau of Investigation to disseminate such information only in conformance with guidelines approved by the Attorney General for foreign intelligence and foreign counterintelligence investigations. If the information is to be disseminated to another federal agency, it can only be disseminated if the information is clearly relevant to the authorized responsibilities of such agency.

Subsection 2709(e) further requires that on a semiannual basis the Director of the Federal Bureau of Investigation 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 by the Bureau under subsection 2709(b).

New section 2710—Definitions for chapter

Terms used in section 2510 retain the definitions given to each term by that section. The term "remote computing service" is defined to mean the provision to the public of computer storage, or computer processing services by means of an electronic communications system.

This section also provides for the change in the table of chapters of title 18 of the United States Code by adding chapter 121 to the table.

Section 202—Effective date

This section provides that the amendments made by Title II of the bill shall be effective 90 days after the date of enactment. It further provides that changes made by this title that apply to conduct pursuant to court order or extension, apply only with respect to court orders or extensions made after the effective date of the title.

TITLE III—PEN REGISTERS AND TRAP AND TRACE DEVICES

Title III of the Electronic Communications Privacy Act proposes to add a new chapter 206 to title 18 of the United States Code. This chapter will govern the use, application and issuance of orders for pen registers and trap and trace devices. Those terms are defined

in proposed section 3126 of title 18. Briefly, a pen register is a device which can be attached to a telephone line for the purpose of decoding and recording the numbers dialed from that line. A trap and trace device is used to identify the originating number of an incoming wire or electronic communication. These devices do not identify or record the contents of the communciation.

Section 301—Pen registers and trap and trace devices

Subsection 301(a) of the Electronic Communications Privacy Act sets out the six proposed sections of title 18 governing pen registers and trap and trace devices.

New section 3121—General prohibition on use of pen registers and trap and trace devices

Subsection (a) of proposed section 3121 of title 18 contains a general prohibition against the installation or use of a pen register or trap and trace device without a court order. Such a court order may be obtained under section 3123 of title 18 or under the Foreign Intelligence Surveillance Act (FISA).

Proposed subsection 3121(b) contains exceptions to subsection (a)'s general prohibition against the use of pen registers and trap and trace devices. Providers of electronic or wire communication services may use pen registers or trap and trace devices if one of three conditions are met. The provider may use a pen register or trap and trace device (1) if it relates to the operation, maintenance, and testing of a wire or elecronic communication service, or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse or unlawful use of the service; (2) to record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward completion, or a user of that service from fraudulent, unlawful or abusive use of service; or (3) where the consent of the user has been obtained.

Proposed subsection 3121(c) imposes a penalty for a knowing violation of subsection (a). The penalty is a fine under this title, imprisonment for up to 1 year, or both.

New section 3122—Applications

Proposed section 3122 of title 18 sets out the procedures for applying for a court order for a pen register or trap and trace device. Under subsection (a), a government attorney may apply for an order, or the extension of an order, authorizing or approving the installation and use of a pen register or trap and trace device. Such order must be made in writing under oath or affirmation to a court of competent jurisdiction.

Proposed paragraph 3122(a)(2) contains parallel provisions for state investigative or law enforcement officers. The phrase "Unless prohibited by state law," makes clear that this law does not preempt any existing state law regulating the installation and use of pen registers or trap and trace devices by state officials. To the extent that state law currently provides that a pen register or trap and trace device may only be installed or used by a state official based on some other, higher standard of proof, that law will continue in effect with respect to such officials.

Proposed subsection 3122(b) of title 18 sets out the contents required in an application for a court order for a pen register or a trap and trace device. The application must include the identity of the applicant and the law enforcement agency conducting the investigation. Also, the applicant must certify that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the agency.

New section 3123—Issuance of orders

Subsection (a) of proposed section 3123 provides that, upon application, a court shall issue an *ex parte* order authorizing the installation and use of a pen register or trap and trace device within its jurisdiction. To issue an order, the court must first be satisfied that the information sought is relevent to an ongoing criminal investigation. This provision does not envision an independent judicial review of whether the application meets the relevance standard, rather the court needs only to review the completeness of the certification submitted.

Proposed paragraph 3123(b)(1) describes the contents of the order authorizing the use or installation of a pen register or trap and trace device. The order shall specify (A) the identity, if known, of the person whose telephone line will receive the pen register; (B) the identity, if known, of the person who is under criminal investigation; (C) the number and, if known, location of the telephone line and, in the case of a trap and trace device, the geographic limits of the order; and (D) a statement of the offense to which the information likely to be obtained relates.

Under proposed paragraph 3123(b)(2), the order, upon request of the applicant, shall direct a third party to furnish information, facilities, and technical assistance necessary to install the pen register or trap and trace device. This provision of the order relating to cooperation is intended to codify the existing informal practice of cooperation between telephone companies and the Department of Justice.

Under proposed subsection 3123(c), the time period of authorization of installation and use of a pen register or a trap and trace device is 60 days, with possible extensions of 60 days. An extension may be granted upon application for a section 3122 order. The same judicial findings required by subsection 3123(a) are also required.

Proposed subsection 3123(d) provides that an order authorizing or approving the installation and use of a pen register or trap and trace device shall direct that the order be sealed, until otherwise ordered by the court. In addition, the order shall bar the disclosure of the existence of the pen register or trap and trace device and the disclosure of an investigation to the listed subscriber or to any other unauthorized person unless or until otherwise directed by the court. Intentional violations of the non-disclosure provisions may be, in appropriate circumstances, punishable as contempt.

New section 3124—Assistance in installation and use

Proposed subsection 3124(a) provides that upon the request of an authorized person, a wire or electronic communication service provider, landlord, custodian, or other person shall furnish such re-

quester with all information, facilities, and technical assistance necessary to effectuate the pen register order unobtrusively and with a minimum of interference. The Committee assumes that the current practice of law enforcement officials installing and maintaining pen registers will continue.

For trap and trace devices, proposed subsection 3124(b) provides that upon request of a government attorney or law enforcement officer authorized to receive the results, a wire or electronic communication service provider, landlord, custodian or other person shall promptly install the trap and trace device and furnish the requester all additional information, facilities and technical assistance, including installation and operation of the device unobtrusively and with a minimum of interference with services, provided that the installation and service is ordered under section 3123(b). This provision also requires that the results be furnished to the law enforcement officer designated by the court, at reasonable intervals, during regular business hours for the duration of the order, unless the court orders otherwise.

Proposed subsection 3124(c) provides reasonable compensation for those providing facilities and assistance under this section. This compensation provision is modeled after that which applies under section 2518 of title 18 and subsection 106(b) of this bill. It is intended to be interpreted and implemented in a similar fashion.

Proposed subsection 3124(d) provides that no cause of action shall lie in any court against a wire or electronic communication service provider, its officers, agents, employees or other specified persons for providing information, assistance or facilities in accordance with the terms of a chapter 206 court order.

Proposed subsection 3124(e) establishes a good faith defense against any civil or criminal action brought under chapter 206 or any other law.

New section 3125—Reports

Under a current order of the Attorney General, statistics concerning pen registers are compiled. Proposed section 3125 requires that this information be reformulated and submitted to the appropriate committees of Congress. It also extends such reporting requirements to trap and trace devices.

Specifically, proposed section 3125 requires that the Attorney General annually report to Congress on the number of pen register and trap and trace device orders applied for by law enforcement agencies of the Department of Justice. The Committee requests that these reports include information as to the nature of the offenses for which the pen registers and trap and trace devices are being used.

New section 3126—Definitions

Proposed section 3126 contains definitions for this chapter. The terms "wire communication," "electronic communication," and "electronic communication service" have the same meanings as in section 2510 of title 18. The term "court of competent jurisdiction" means (A) a district court of the United States (including a magistrate of such court) or a U.S. Court of Appeals; or (B) a state court

of general criminal jurisdiction authorized to enter pen register or trap and trace orders.

As indicated in proposed section 3126(3), the term "pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted for purposes of routing telephone calls, with respect to wire communications, on the telephone line to which such device is attached. Pen registers do not record the contents of a communication. They record only the telephone numbers dialed.

Devices used by a provider or customer or wire or electronic communication service incident to billing or cost accounting, or for any other similar purposes in the ordinary course of business are excluded from the definition of a pen register. Thus, devices that many companies and firms use to record billable time for their clients' accounts are outside this bill's prohibitions against the installation and use of pen registers.

Trap and trace devices are defined in proposed subsection 3126(4). A "trap and trace device" is a device which captures the incoming electronic or other impulses which identify the originating number of an incoming wire or electronic communication. Trap and trace devices do not record the contents of communications.

The term "attorney for the government" has the meaning given to that term by the Federal Rules of Criminal Procedure. The term "State" means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.

Subsection 301(b) of the bill contains a clerical amendment to the table of chapters.

Section 302—Effective date

Section 302 of the bill contains the effective date for Title III of the Electronic Communications Privacy Act. Subsection (a) provides that as a general rule, Title III of the bill shall take effect 90 days after enactment. In the case of conduct pursuant to a court order or extension, these amendments apply only with respect to court orders or extensions made after this title takes effect. Subsection 302(b) of the bill contains special rules which, in essence, give states two years to bring their laws into conformity with the Electronic Communications Privacy Act's amendments to Federal law.

Section 303—Interference with the operation of a satellite

This section of the bill adds a new section to chapter 65 of title 18, United States Code.

New section 1367—Interference with the operation of a satellite

Subsection (a) of this proposed section provides that anyone who, without the authority of the satellite operator, intentionally or maliciously interferes with the authorized operation of a satellite or obstructs or hinders any satellite transmission, including both the transmission from the ground to the satellite and the transmission from the satellite to the ground (commonly known as the up-link and the down-link respectively) is subjected to criminal penalties including a fine of up to $250,000, imprisonment for not more than 10 years, or both. The subsection does not prohibit any actions by

the authorized satellite operator which are designed to protect the satellite from unauthorized use.

Subsection (b) of this new section makes it clear that the criminal act described in subsection (a) does not include any lawfully authorized investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the United States. This subsection does not provide any new authority for such activities.

Finally, this section of the bill provides that the table of sections for chapter 65 of title 18 is amended to include the new section 1367.

VI. Agency Views

On June 25, 1986 and July 29, 1986, the Committee received the following letters from the Department of Justice.

U.S. Department of Justice,
Office of Legislative and Intergovernmental Affairs,
Washington, DC, June 25, 1986.

Hon. Strom Thurmond,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

Dear Mr. Chairman: This letter is to advise you of the Department of Justice's position with regard to S. 2575, the Electronic Communications Privacy Act of 1986. This bill, which is identical to H.R. 4952 as recently passed by the House of Representatives, makes important changes to the existing wiretap statutes and fills gaps in current laws by creating provisions to regulate interception of and access to new forms of electronic communication such as data transmissions.

The Department of Justice has worked intensively on this legislation over the past several weeks with the staff of the Subcommittee on Patents, Copyrights and Trademarks, as well as with interested representatives of industry and civil liberties groups. While initial versions of this legislation did not in our view adequately safeguard legitimate and vital law enforcement and national security needs for access to communications, as a result of the negotiations that have occurred the bill has been substantially modified to accommodate our concerns. In our judgment the bill as presently drafted fairly balances the interests of privacy and law enforcement and its enactment would represent a major accomplishment of the 99th Congress, holding forth the promise of significant benefits for business, privacy, and law enforcement alike.

Accordingly, the Department of Justice strongly supports the enactment of S. 2575.

Sincerely,

John R. Bolton,
Assistant Attorney General.

U.S. DEPARTMENT OF JUSTICE,
OFFICE OF LEGISLATIVE AND
INTERGOVERNMENTAL AFFAIRS,
Washington, DC, 20530 July 29, 1986.

Hon. STROM THURMOND,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: This is with further reference to my letter of June 25, 1986, expressing support for S. 2575, the Electronic Communications Privacy Act of 1986. A copy of my earlier letter is enclosed for ready reference.

We continue to believe that this measure is a well balanced one which, in addition to modernizing the 1968 electronic surveillance law, also benefits both law enforcement and individual privacy by clarifying many aspects of this highly complex area of the law. As the 99th Congress is rapidly drawing to a close, we sincerely hope that the Senate will act on S. 2575 at an early date.

We would deeply appreciate your consideration of S. 2575 and, if possible, your formal co-sponsorship of the bill. Having your name on the bill would, we believe, be most helpful in efforts to process this important legislation this year.

Sincerely,

JOHN R. BOLTON,
Assistant Attorney General.

VII. COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, September 23, 1986.

Hon. STROM THURMOND,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has reviewed S. 2575, the Electronic Communications Privacy Act of 1986, as ordered reported by the Senate Committee on the Judiciary, September 19, 1986. CBO estimates that enactment of this legislation would result in no significant cost to the federal government and in no cost to state or local governments.

S. 2575 would make a number of amendments to Title 18 of the U.S. Code concerning access to electric communications. Title I of the bill would establish penalties for the unlawful interception or disclosure of electronic communications, provide for the recovery of civil damages for persons whose communications are intercepted, disclosed or used in violation of this provision, and modify procedures for government interception of communications. Title II would create specific penalties for unlawful access to stored wire and electronic communications, while Title III would establish a general prohibition on the use of pen registers. These titles would mandate specific procedures for access to stored communications and use of pen registers by government entities, and Title II would allow for civil actions.

S. 2575 would require government entities to compensate private parties assembling or providing information concerning stored electronic communications, or assisting in the installation and use of a pen register. Because such compensation is currently provided in Department of Justice (DOJ) investigations, CBO does not expect the these provisions would result in any significant additional cost to the federal government.

Based on information from the DOJ, we do not expect that enactment of this bill would result in a significant change in the government's law enforcement practices or expenditures. S. 2575 would specifically authorize law enforcement efforts the DOJ is currently undertaking with other authority.

If you wish further details on this estimate, we will be pleased to provide them.

With best wishes,

Sincerely,

JAMES BLUM
(for Rudolph G. Penner, Director).

VIII. REGULATORY IMPACT STATEMENT

In compliance with paragraph 11(b) of Rule XXVI of the Standing Rules of the Senate, the Committee has concluded that no significant additional regulatory impact would be incurred in carrying out the provisions of this legislation. After due consideration, the Committee concluded that the changes in existing law contained in the bill will not increase or diminish any present regulatory responsibilities of the U.S. Department of Justice or any other department or agency affected by the legislation.

IX. VOTE OF COMMITTEE

On August 12, 1986, the Subcommittee on Patents, Copyrights, and Trademarks, with a quorum present, reported S. 2575, with an amendment in the nature of a substitute, to the Committee on the Judiciary by voice vote. On September 19, 1986, the Judiciary Committee adopted two further changes in the bill as reported by the Subcommittee. The Judiciary Committee, with a quorum present, and without objection heard, approved the amendment in the nature of a substitute. The Committee then favorably reported S. 2575, as amended, by unanimous consent.

X. CHANGES IN EXISTING LAW

In compliance with paragraph 12 of Rule XXVI, of the Standing Rules of the Senate, changes in existing law made by S. 2575 as reported are shown as follows (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

* * * * * * *

TITLE 18—CRIMES AND CRIMINAL PROCEDURE

PART I. CRIMES

PART II—CRIMINAL PROCEDURE

CHAPTER 65—MALICIOUS MISCHIEF

§ 1367. Interference with the operation of a satellite

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

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

* * * * * * *

CHAPTER 109—SEARCHES AND SEIZURES

* * * * * * *

§ 2232. Destruction or removal of property to prevent seizure

(a) PHYSICAL INTERFERENCE WITH SEARCH.—Whoever, before during, or after seizure of any property by any person authorized to make searches and seizures, in order to prevent the seizure or securing of any goods, wares, or merchandise by such person, staves, breaks, throws overboard, destroys, or removes the same, shall be fined not more than $10,000 or imprisoned more than five years, or both.

(b) NOTICE OF SEARCH.—Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any perosn, goods, wares, merchandise or other property, gives notice or attempts to give notice of the possible search or seizure to any person shall be fined not more than $10,000 or imprisoned not more than five years, or both.

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

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

* * * * * * *

CHAPTER 119—WIRE *AND ELECTRONIC COMMUNICATIONS* INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

§ 2510. Definitions

As used in this chapter—

(1) "wire communication" means any [communication] *aural transfer* made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (*including the use of such con-*

nection in a switching station) furnished or operated by any person engaged [as a common carrier] in providing or operating such facilities for the transmission of interstate or foreign communications *or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;*

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, *but such term does not include any electronic communication;*

* * * * * * *

(4) "intercept" means the aural *or other* acquisition of the contents of any wire, *electronic*, or oral communication through the use of any electronic, mechanical, or other device.

(5) "electronic mechanical, or other device" means any device or apparatus which can be used to intercept a wire [or oral], *oral, or electronic* communication other than—

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a [*communications common carrier*] *provider of wire or electronic communication service* in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business *or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business*; or (ii) being used by a communications common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

* * * * * * *

(8) "contents", when used with respect to any wire [or oral], *oral, or electronic* communication, includes any information concerning the [identity of the parties to such communication or the existence,] substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means—

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire [or oral], *oral, or electronic* communications;

(10) "communication common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) of title 47 of the United States Code; [and]

(11) "aggrieved person" means a person who was a party to any intercepted wire [or oral], *oral, or electronic* communication or a person against whom the interception was directed[.];

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

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

(B) any wire or oral communication;

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

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

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

(A) uses an electronic communication service; and

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

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

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

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

(A) scrambled or encrypted;

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

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

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

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

(17) "electronic storage" means—

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

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

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

§ 2511. Interception and disclosure of wire or oral communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who—

(a) [willfully] *intentionally* intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire [or oral] *oral, or electronic* communication;

(b) [willfully] *intentionally* uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the permises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) [willfully] *intentionally* discloses, or endeavors to disclose, to any other person the contents of any wire [or oral] *oral, or electronic* communication, knowing or have reason to know that the information was obtained through the interception of a wire [or oral] *oral, or electronic* communication in violation of this subsection; or

(d) [willfully] *intentionally* uses, or endeavors to use, the contents of any wire [or oral] *oral, or electronic* communication, knowing or having reason to know that the information was obtained through the interception of a wire [or oral] *oral, or electronic* communication in violation of this subsection; [shall be fined not more than $10,000 or imprisoned not more than five years, or both.] *shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).*

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of [any communication common carrier,] *a provider of wire or electronic com-*

munication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property [of the carrier of such communication: *Provided,* That said communication common carriers] *of the provider of that service, except that a provider of wire communication service to the public* shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, *providers of wire or electronic communication service,* [communication common carriers,] their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information facilities, or technical assistance to persons authorized by law to intercept wire [or oral], *oral, or electronic* communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if [the common carrier,] *such provider* its officers, employees, or agents, landlord, custodian, or other specified person has been provided with—

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required.

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No [communication common carrier] *provider of wire or electronic communication service* officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished an order or certification under this subparagraph, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivsion of a State, as may be appropriate. Any [violation of this subparagraph by a communication common carrier or an officer, employee, or agent thereof] *such disclosure,* shall render [the carrier] *such person* liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any [communication common carrier] *provider of wire or electronic communication service* its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of [an order of certification under this subparagraph] *a court order or certification under this chapter.*

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforce-

ment of chapter 5 of title 57 of the United States Code, to intercept a wire or *electronic* communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire [or oral], *oral, or electronic* communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire [or oral], *oral, or electronic,* communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State [or for the purpose of committing any other injurious act].

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an office, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or *chapter 121,* or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communication [by], *or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing* a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.

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

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

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

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

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

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

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the

offense under paragraph (a) is a radio communication that is not scrambled or encrypted, then—

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

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

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

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

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

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

(5)(a)(i) If the communication is—

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

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

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

(ii) In an action under this subsection—

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

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

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

§ 2512. Manufacture, distribution, possession, and advertising of wire or oral communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who [willfully] *intentionally*—

(a) sends through the mail, or sends or carriers in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications;

(b) manufacturers, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication any advertisement of—

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications,

knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for—

(a) [a communications common carrier] *a provider of wire or electronic communication service* or an officer, agent, or employee of, or a person under contract with, [a communications common carrier] *such a provider,* in the normal course of the [communications common carrier's business] *business of providing that wire or electronic communication service,* or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications.

§ 2513. Confiscation of wire [or oral], *oral, or electronic* communication intercepting devices

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose of the Attorney General.

§ 2515. Prohibition of use as evidence of intercepted wire [or oral], *oral, or electronic* communications

Whenever any wire [or oral], *oral, or electronic* communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

§ 2516. Authorization for interception of wire [or oral], *oral, or electronic* communications

(1) The Attorney General, Deputy Attorney General, Assoicate Attorney General, [or] any Assistant Attorney General, *any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division* specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire of oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—

(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of

the Atomic Energy Act of 1954), *section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel),* or under the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relating to sabotage), chapter 115 (relating to treason), [or] chapter 192 (relating to riots), *chapter 65 (relating to malicious matter mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy);*

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murders, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 224 (bridery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1084 (transmission of wagering information), *section 751 (relating to escape),* sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assualt), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transporation in aid of racketeering enterprises), section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire), section 1952B (relating to violent crimes in aid of racketeering activity), section 1954 (offer acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 2252 or 2253 (sexual exploitation of children), Section 2251 and 2252 (sexual exploitation of children), section [2314] *2312, 2313, 2314,* and 2315 (interstate transportation of stolen property), *the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities),* section 1963 violations with respect to racketeer influenced and corrupt organizations), *section 115 (relating to threatening or retaliating against a Federal official), the section in chapter 65 relating to destruction of an energy facility, and section 1341 (relating to mail fraud),* [or] section 351 (volations with respect to congressional, Cabinet, or Supreme Court assissination, kidnapping, and assault), *section 831 (relating to prohibited transaction involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), or section 1992 (relating to wrecking trains);*

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions); [or]

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

(i) any violation of section 1679(c)(2) (relating to destruction of a natural gas pipeline) or subsection (i) or (n) of the United States Code;

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

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

[(h)](*l*) any conspiracy to commit any of the foregoing offenses.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire [or oral], *oral, or electronic* communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire [or oral], *oral, or electronic* communications by investigative or law enforcement of officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

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

§ 2517. Authorization for disclosure and use of intercepted wire [or oral], *oral, or electronic* communication

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire [or oral], *oral, or electronic* communication,

or evidence derived therefrom may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire [or oral], *oral, or electronic* communication or evidence derived therefrom any use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire [or oral], *oral, or electronic* communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire [or oral], *oral, or electronic* communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire or oral communications in the manner authorized herein, intercepts wire [or oral], *oral, or electronic* communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

§ 2518. Procedure for interception of wire [or oral], *oral, or electronic* communications

(1) Each application for an order authorizing or approving the interception of a wire [or oral], *oral, or electronic* communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) *except as provided in subsection (11),* a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought

to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire [or oral], *oral, or electronic* communications involving any of the same persons, facilities or places specified in the application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire [or oral], *oral, or electronic* communications within the territorial jurisdiction of the court in which the judge is sitting *(and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction)* if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter.

(b) there is probable cause for brief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) *except as provided in subsection (11),* there is probable cause for belief that the facilities from which, or the place where the wire [or oral], *oral, or electronic* communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire [or oral], *oral, or electronic* communication under this chapter shall specify—

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire [or oral], *oral, or electronic* communication under this chapter shall, upon request of the applicant, direct that a [communication common carrier], *provider of wire or electronic communication service,* landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such [carrier] *service provider,* landlord, custodian, or person is according the person whose communications are to be intercepted. Any [communication common carrier] provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant [at the prevailing rates.] *for reasonable express incurred in providing such facilities or assistance.*

(5) No order entered under this section may authorize or approve the interception of any wire [or oral], *oral, or electronic* communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. *Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered.* Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise, subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. *In the event the intercepted communications is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Goverment personnel, or by an individual operating under a contract with the Government,*

acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant of that State, who reasonably determines that—

(a) an emergency situation exists that involves—

(i) immediate danger of death or serious physical injury to any person.

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime,

that requires a wire [or oral], *oral, or electronic* communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception.

may intercept such wire [or oral], *oral, or electronic* communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire [or oral], *oral, or electronic* communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8)(a) The contents of any wire [or oral], *oral, or electronic* communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire [or oral], *oral, or electronic* communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under this directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this sub-

section, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire [or oral], *oral, or electronic* communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of—

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

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire [or oral], *oral, or electronic* communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire [or oral], *oral, or electronic* communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less then ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that—

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

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

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

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

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

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

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

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

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

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

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

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

§ 2519. Reports concerning intercepted wire [or oral], *oral, or electronic* communications

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for (*including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2581(3)(d) of this title did not apply by reason of section 2518(11) of title*);

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

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension or an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts—

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

(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, and (iv) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

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

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire [or oral], *oral, or electronic* communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

§ 2520. Recovery of civil damages authorized

[Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications, and (2) be entitled to recover from any such person—

[(a) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;

[(b) punitive damages; and

[(c) a reasonable attorney's fee and other litigation costs reasonably incurred.

A good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under this chapter or under any other law.]

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

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

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

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

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

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

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

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1,000.

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

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

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

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

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

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

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

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

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

§ 2521. Injunction against illegal interception

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon a practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons

for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the federal Rules of Criminal Procedure.

* * * * * * *

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

§ 2701. Unlawful access to stored communications

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 2702. Disclosure of contents

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 2703. Requirements for governmental access

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

(b) CONTENTS OF ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any

electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) of this section shall issue only if the governmental entity shows that there is reason to believe the con-

tents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminious in nature or compliance with such order otherwise would cause an undue burden on such provider.

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

§ 2704. Backup preservation

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

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

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

(A) the delivery of the information; or

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

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

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

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

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

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

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

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

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

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

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

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

§ 2705. Delayed notice

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

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

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

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

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

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

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

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

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

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

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

(B) informs such customer or subscriber—

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

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

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

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

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

(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

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

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

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

§ 2706. Cost reimbursement

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

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

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

§ 2707. Civil action

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

entity which engaged in that violation such relief as may be appropriate.

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

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

(2) damages under subsection (c); and

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

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

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

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

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

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

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

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

§ 2708. Exclusivity of remedies

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

§ 2709. Counterintelligence access to telephone toll and transactional records

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

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

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

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

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

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

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

§ 2710. Definitions for chapter

As used in this chapter—

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

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

* * * * * * *

CHAPTER 205—SEARCHES AND SEIZURES

§ 3117. Mobile tracking devices

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

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

CHAPTER 206—PEN REGISTERS AND TRAP AND TRACE DEVICES

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

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

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

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

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

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

(a) APPLICATION.—(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

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

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

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

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

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

(a) IN GENERAL.—Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device

within the jurisdiction of the court if the court finds that the attorney for the Government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

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

(1) shall specify—

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

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

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

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

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

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

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

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

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

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

§ 2124. Assistance in installation and use of a pen register or a trap and trace device

(a) PEN REGISTERS.—Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively

and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

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

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

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

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

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

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

§ 3126. Definitions for chapter

As used in this chapter—

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

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

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

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

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

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

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

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

○