

Notes from Eric Poole, Sysop of Leo Technology BBS:

-----  
Over the last couple of weeks, I've been calling around to CompuServe, the Circuit Cellar INK BBS, and everywhere else I can think of, trying to find the full text of the Electronic Communications Privacy Act of 1986. The best I've been able to come up with so far are some excerpts from the preliminary House of Representatives version.

Last night, October 7, 1988, someone (whose name I would like to include here but I haven't yet gotten his permission to do so) called the Leo Technology BBS for the first time out of the clear blue sky, long distance from Washington to New Hampshire on his own nickel, went through all the new-user questionnaires and stuff, and uploaded the full text of the act, all hundred-some-odd-thousand bytes of it. So, here it is. Thanks to the provider, (I'm sure it'd be OK to put his name here, but like I said, I didn't yet get his permission to do so); it's guys like you that make all this BBS sysoping stuff worth while!

I believe the contents of this file to be accurate, however, please, before taking any action or making any decisions based upon what you read in this file, CONFIRM THE LANGUAGE IN THIS FILE AGAINST AN OFFICIAL LEGAL SOURCE, and if you aren't a lawyer, go get one.

Eric Poole, CIS 73127,2034  
Sysop, Leo Technology BBS, Londonderry, NH  
(603) 432-2517 300-1200-2400 8-N-1  
7 days 24 hrs Full & free access first call

\* \* \* \* \*

0188ibm021  
February 2, 1987 (originally)  
March 9, 1988 (reprint)

## TITLE 18 - CRIMES AND CRIMINAL PROCEDURE

### PART I. CRIMES

| Chapter   | Sec. |
|---|------|
| General provisions . . . . .  | 1    |
| 119. Wire and electronic communications interception and interception of oral communications 2510 |      |
| 121. Stored Wire and Electronic Communications and Transactional Records Access 2701              |      |

### PART II. CRIMINAL PROCEDURE

|   |      |
|---|------|
| 201. General provisions . . . . .                       | 3001 |
| 206. Pen Registers and Trap and Trace Devices . . . . . | 3121 |

## CHAPTER 65 - MALICIOUS MISCHIEF

Sec.

1367. Interference with the operation of a satellite.

\_ 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 person, 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 \$100,000 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

Sec.

- 2510. Definitions.
- 2511. Interception and disclosure of wire or oral communications prohibited.
- 2512. Manufacture, distribution, possession, and advertising of wire or oral communication intercepting devices prohibited.
- 2513. Confiscation of wire, oral, or electronic communication intercepting devices.
- 2514. Immunity of witnesses.
- 2515. Prohibition of use as evidence of intercepted wire, oral, or electronic communications.
- 2516. Authorization for interception of wire, oral, or electronic communications.
- 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications.
- 2518. Procedure for interception of wire, oral, or electronic communications.
- 2519. Reports concerning intercepted wire, oral or electronic communications.
- 2520. Recovery of civil damages authorized.
- 2521. Injunction against illegal interception.

\_ 2510. Definitions

As used in this chapter --

- (1) "wire communication" means any 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 connection in a switching station) furnished or operated by any person engaged 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;

- (3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.
- (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, 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 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;
  - (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;
- (6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;
- (7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;
- (8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the 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, 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;
- (11) "aggrieved person" means a person who was a party to any intercepted wire, 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, oral, or electronic communications prohibited

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

- (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
- (b) 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 premises 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) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or have reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or
- (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

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 a provider of wire or electronic communication 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 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, 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, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if 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 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 a court order or certification under this chapter, 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 subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any 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 or certification under this subparagraph.

- (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 enforcement of chapter 5 of title 47 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, 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, 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.
- (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 officer, 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 communications, 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 or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.
- (3) (a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.
- (b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication --
  - (i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;
  - (ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;
  - (iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or
  - (iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.
- (4) (a) Except as provided in paragraph (b) of this subsection or in

subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

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

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

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

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

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

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

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

- (5) (a) (i) If the communication is --

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

- (B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not

for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain.

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

(ii) In an action under this subsection --

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

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

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

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

(1) Except as otherwise specifically provided in this chapter, any person who intentionally --

(a) sends through the mail, or sends or carries 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, oral, or electronic communications;

(b) manufactures, 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, 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, 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, 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 provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communications 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, oral, or electronic communications.

\_ 2513. Confiscation of wire, 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 by the Attorney General.

\_ 2515. Prohibition of use as evidence of intercepted wire or oral communications

Whenever any wire or oral 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, oral, or electronic communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, 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 or 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), chapter 102 (relating to riots), chapter 65 (relating to malicious 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 (bribery 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 assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation 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 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), 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), sections 2251 and 2252 (sexual exploitation of children), sections 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), section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), or section 1992 (relating to wrecking trains);
- (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);
  - (h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;
  - (i) any violation of section 1679a(c)(2) (relating to destruction of a natural gas pipeline) or subsection (i) or (n) of section 1472 (relating to aircraft piracy) of title 49, of the United States Code;
  - (j) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act); or
  - (k) the location of any fugitive from justice from an offense described in this section;
  - (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, 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, oral, or electronic communications by investigative or law enforcement 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, or order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense 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, oral, or electronic communications

- (1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, 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, oral, or electronic communication or evidence derived therefrom may 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, 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, 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, oral, or electronic communications in the manner authorized herein, intercepts wire, 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, oral, or electronic communications

- (1) Each application for an order authorizing or approving the interception of a wire, 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, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such 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, 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 belief 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, 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, 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, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a 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 service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any 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 for reasonable expenses incurred in providing such facilities or assistance.

- (5) No order entered under this section may authorize or approve the interception of any wire, 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 communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.
- (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 to a statute 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, 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, 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, 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, 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, oral, or electronic communication under this subsection shall be done in such 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 his 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 subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, 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, and 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, 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, 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 than 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, oral, or electronic 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, oral, or electronic 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 subsection, 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 this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if --
- (a) in the case of an application with respect to the interception of an oral communication --
    - (i) the application is by a federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;
    - (ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and
    - (iii) the judge finds that such specification is not practical; and
  - (b) in the case of an application with respect to a wire or electronic communication --
    - (iv) 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;

(v) 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

(vi) 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, 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 2518(3)(d) of this title did not apply by reason of section 2518(11) of this 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 of 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, 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

- (a) IN GENERAL.--Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.
- (b) RELIEF.--In an action under this section, appropriate relief includes--
  - (1) such preliminary and other equitable or declaratory relief as may be appropriate;
  - (2) damages under subsection (c) and punitive damages in appropriate cases; and
  - (3) a reasonable attorney's fee and other litigation costs reasonably incurred.
- (c) COMPUTATION OF DAMAGES. --
  - (1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:
    - (A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) 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 as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the federal Rules of Criminal Procedure.

#### CHAPTER 121- STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

##### Sec.

2701. Unlawful access to stored communications.

2702. Disclosure of contents.

2703. Requirements for governmental access.

2704. Backup preservation.

2705. Delayed notice.

2706. Cost reimbursement.

2707. Civil action.

2708. Exclusivity of remedies.

2709. Counterintelligence access to telephone toll and

transactional records.

2710. Definitions

2701. Unlawful access to stored communications

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

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

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

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

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

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

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

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

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

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

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

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

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

\_ 2702. Disclosure of contents

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

- (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
  - (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--
    - (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and
    - (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.
- (b) EXCEPTIONS.-- A person or entity may divulge the contents of a communication--
- (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
  - (2) as otherwise authorized in section 2516, 2511(2)(a), or 2703 of this title;
  - (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
  - (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;
  - (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or
  - (6) to a law enforcement agency, if such contents--
    - (A) were inadvertently obtained by the service provider; and
    - (B) appear to pertain to the commission of a crime.

\_ 2703. Requirements for governmental access

- (a) CONTENTS OF ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.-- A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less,

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

(b) CONTENTS OF ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.--

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

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

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

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

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

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

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

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

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

(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.--

(1) (A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications

covered by subsection (a) or (b) of this section) to any person other than a governmental entity.

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

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

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

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

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

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

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

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

#### \_ 2704. Backup preservation

(a) BACKUP PRESERVATION.--

- (1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.
- (2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).
- (3) The service provider shall not destroy such backup copy until the later of--
  - (A) the delivery of the information; or
  - (B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.
- (4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider--
  - (A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and
  - (B) has not initiated proceedings to challenge the request of the governmental entity.
- (5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

(b) CUSTOMER CHALLENGES.--

- (1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion



to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement--

- (A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and
  - (B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.
- (2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure.
  - (3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.
  - (4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.
  - (5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

\_ 2705. Delayed notice

(a) DELAY OF NOTIFICATION.--

- (1) A governmental entity acting under section 2703(b) of this title may--
  - (A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or
  - (B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.
- (2) An adverse result for the purposes of paragraph (1) of this subsection is--
  - (A) endangering the life or physical safety of an individual;
  - (B) flight from prosecution;
  - (C) destruction of or tampering with evidence;
  - (D) intimidation of potential witnesses; or
  - (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.
- (3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).
- (4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.
- (5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that--

- (A) states with reasonable specificity the nature of the law enforcement inquiry; and
- (B) informs such customer or subscriber--
  - (i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;
  - (ii) that notification of such customer or subscriber was delayed;
  - (iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and
  - (iv) which provision of this chapter allowed such delay.
- (6) As used in this subsection, the term "supervisory official" means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.
- (b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.-- A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will results in--
  - (1) endangering the life or physical safety of an individual;
  - (2) flight from prosecution;
  - (3) destruction of or tampering with evidence;
  - (4) intimidation of potential witnesses; or
  - (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

- (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

Sec. 3101. Effect of rules of court--Rules

3117. Mobile tracking devices.

\_ 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 TRACE DEVICES

Sec.

- 3121. General prohibition on pen register on trap and trace device use; exception.
- 3122. Application for an order for a pen register or a trap and trace device.
- 3123. Issuance of an order for a pen register or a trap or trace device.
- 3124. Assistance in installation and use of a pen register or a trap and trace device.
- 3125. Reports concerning pen registers and trap and trace devices.
- 3126. Definitions for chapter.

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

- (a) In General.-Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).
- (b) Exception.-The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service-
  - (1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or
  - (2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or with the consent of the user of that service.
- (c) Penalty.-Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

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

(a) Application.-

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

(b) Contents Of Application. - An application under subsection (a) of this section shall include-

- (1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and
- (2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

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

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

(b) Contents Of Order.-An order issued under this section-

(1) shall specify-

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



- (C) the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and
    - (D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and
  - (2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.
- (c) Time Period And Extensions.-
- (1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.
  - (2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.
- (d) Nondisclosure Of Existence Of Pen Register Or A Trap And Trace Device.-An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that-
- (1) the order be sealed until otherwise ordered by the court; and
  - (2) the person owning or leasing the line to which the pen register or a trap and trace device is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

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

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

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

- (b) Trap And Trace Device.-Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 3123(b)(2) of this title. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished to the officer of a law enforcement agency, designated in the court, at reasonable intervals during regular business hours for the duration of the order.
- (c) Compensation.-A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.
- (d) No Cause Of Action Against A Provider Disclosing Information Under This Chapter.-No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order under this chapter.
- (e) Defense.-A good faith reliance on a court order, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law.

\_ 3125. Reports concerning pen registers and trap and trace devices

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

\_ 3126. Definitions for chapter

As used in this chapter-

- (1) the terms "wire communication", "electronic communication", and "electronic communication service" have the meanings set forth for such terms in section 2510 of this title;
- (2) the term "court of competent jurisdiction" means-
  - (A) a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals; or
  - (B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;
- (3) the term "pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;
- (4) the term "trap and trace" device means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted;
- (5) the term "attorney for the Government" has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and
- (6) the term "State" means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.