(g) **Defense.** In a prosecution under this section based on illicit sexual conduct as defined in subsection (f)(2), it is a defense, which the defendant must establish by a preponderance of the evidence, that the defendant reasonably believed that the person with whom the defendant engaged in the commercial sex act had attained the age of 18 years.

18 U.S.C. § 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;

(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 provider of wire or electronic communication service 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'' has the meaning given that term in section 3 of the Communications Act of 1934;

(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) any wire or oral communication;

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

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

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(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 wire or 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;

(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;

(19) ''foreign intelligence information'', for purposes of section 2517(6) of this title, means—

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States;

(20) ''protected computer'' has the meaning set forth in section 1030; and

(21) ''computer trespasser''—

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

18 U.S.C. § 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 having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(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; or

(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)–(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

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 or electronic 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 or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978 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 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 a court order, statutory authorization, or certification under this chapter.

(iii) If a certification under subparagraph (ii)(B) for assistance to obtain foreign intelligence information is based on statutory authority, the certification shall identify the specific statutory provision and shall certify that the statutory requirements have been met.

(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 206 of this title, 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 or chapter 121 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, oral, and electronic 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.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if—

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(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) 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.

18 U.S.C. § 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 or disseminates by electronic means any advertisement of—

(i) any electronic, mechanical, or other device knowing the content of the advertisement and 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 the content of the advertisement and 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 under this title 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 communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof,

to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device.

18 U.S.C. § 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.

18 U.S.C. § 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.

18 U.S.C. § 2516. AUTHORIZATION FOR INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security 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 2122 and 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 10 (relating to biological weapons), chapter 37 (relating to espionage), chapter 55 (relating to kidnapping), chapter 90 (relating to protection of trade secrets), 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 murder, 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 37 (relating to violence at international airports), section 43 (relating to animal enterprise terrorism), section 81 (arson within special maritime and territorial jurisdiction), section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsec-

tion (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 832 (relating to nuclear and weapons of mass destruction threats), section 842 (relating to explosive materials), section 930 (relating to possession of weapons in Federal facilities), section 1014 (relating to loans and credit applications generally; renewals and discounts), section 1114 (relating to officers and employees of the United States), section 1116 (relating to protection of foreign officials), 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 1591 (sex trafficking of children by force, fraud, or coercion), 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 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (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 1344 (relating to bank fraud), section 1992 (relating to terrorist attacks against mass transportation), sections 2251 and 2252 (sexual exploitation of children), section 2251A (selling or buying of children), section 2252A (relating to material constituting or containing child pornography), section 1466A (relating to child obscenity), section 2260 (production of sexually explicit depictions of a minor for importation into the United States), sections 2421, 2422, 2423, and 2425 (relating to transportation for illegal sexual activity and related crimes), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 2340A (relating to torture), 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 38 (relating to aircraft parts fraud), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal official), section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse), 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), section 175 (relating to biological weapons), section 175c (relating to variola virus), section 956 (conspiracy to harm persons or property overseas), a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), or section 1546 (relating to fraud and misuse of visas, permits, and other documents);

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

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

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

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions), or section 5324 of title 31, United States Code (relating to structuring transactions to evade reporting requirement prohibited);

(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 felony violation of chapter 71 (relating to obscenity) of this title;

(j) any violation of section 60123(b) (relating to destruction of a natural gas pipeline), section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with dangerous weapon), or section 46505(b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life, by means of weapons on aircraft) of title 49;

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

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

(m) a violation of section 274, 277, or 278 of the Immigration and Nationality Act (8 U.S.C. 1324, 1327, or 1328) (relating to the smuggling of aliens);

(n) any felony violation of sections 922 and 924 of title 18, United States Code (relating to firearms);

(*o*) any violation of section 5861 of the Internal Revenue Code of 1986 (relating to firearms);

(p) a felony violation of section 1028 (relating to production of false identification documents), section 1542 (relating to false statements in passport applications), section 1546 (relating to fraud and misuse of visas, permits, and other documents), section 1028A (relating to aggravated identity theft) of this title or a violation of section 274, 277, or 278 of the Immigration and Nationality Act (relating to the smuggling of aliens); or

(q) any criminal violation of section 229 (relating to chemical weapons) or sections 2332, 2332a, 2332b, 2332d, 2332f, 2332g, 2332h, 2339, 2339A, 2339B, 2339C, or 2339D of this title (relating to terrorism);

(r) any criminal violation of section 1 (relating to illegal restraints of trade or commerce), 2 (relating to illegal monopolizing of trade or commerce), or 3 (relating to illegal restraints of trade or commerce in territories or the District of Columbia) of the Sherman Act (15 U.S.C. 1, 2, 3); or

(s) any conspiracy to commit any offense described in any subparagraph of this paragraph.

(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, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

18 U.S.C. § 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.

(6) Any investigative or law enforcement officer, or attorney for the Government, 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 any other

Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(7) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, 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 or derivative evidence to a foreign 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, and foreign investigative or law enforcement officers may use or disclose such contents or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

(8) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, 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 or derivative evidence to any appropriate Federal, State, local, or foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

18 U.S.C. § 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. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability

and capacity requirements under the Communications Assistance for Law Enforcement Act.

(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 a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under 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, an inventory which shall include notice of—

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

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

(3) the fact that during the period wire, 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 or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that—

(i) the communication was unlawfully intercepted;

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

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

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in

violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this 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—

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

(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable

cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;

(iii) the judge finds that such showing has been adequately made; and

(iv) the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

(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)(a) shall not begin until 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.

18 U.S.C. § 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, (iv) the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted pursuant to such order, and (v) 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.

18 U.S.C. § 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, other than the United States, 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 $1000.

(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) or 2511(2)(i) 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.

(f) **Administrative discipline.** If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(g) **Improper disclosure is violation.** Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).

18 U.S.C. § 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.

18 U.S.C. § 2522. ENFORCEMENT OF THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT

(a) **Enforcement by court issuing surveillance order.** If a court authorizing an interception under this chapter, a State statute, or the

Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or authorizing use of a pen register or a trap and trace device under chapter 206 or a State statute finds that a telecommunications carrier has failed to comply with the requirements of the Communications Assistance for Law Enforcement Act, the court may, in accordance with section 108 of such Act, direct that the carrier comply forthwith and may direct that a provider of support services to the carrier or the manufacturer of the carrier's transmission or switching equipment furnish forthwith modifications necessary for the carrier to comply.

(b) **Enforcement upon application by Attorney General.** The Attorney General may, in a civil action in the appropriate United States district court, obtain an order, in accordance with section 108 of the Communications Assistance for Law Enforcement Act, directing that a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services comply with such Act.

(c) **Civil penalty.—**

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

(2) *Considerations.* In determining whether to impose a civil penalty and in determining its amount, the court shall take into account—

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

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

(C) such other matters as justice may require.

(d) **Definitions.** As used in this section, the terms defined in section 102 of the Communications Assistance for Law Enforcement Act have the meanings provided, respectively, in such section.

18 U.S.C. § 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;

9-7.302 Consensual Monitoring -- "Procedures for Lawful, Warrantless Monitoring of Verbal Communications"
9-7.400 Defendant Motion or Discovery Request for Disclosure of Defendant Overhearings and Attorney Overhearings
9-7.500 Prior Consultation with the Computer Crime and Intellectual Property Section of the Criminal Division (CCIPS) for Applications for Pen Register and Trap and Trace Orders Capable of Collecting Uniform Resource Locators (URLs)

9-7.010 Introduction

This chapter contains Department of Justice policy on the use of electronic surveillance. The Federal electronic surveillance statutes (commonly referred to collectively as "Title III") are codified at 18 U.S.C. § 2510, *et seq*. Because of the well-recognized intrusive nature of many types of electronic surveillance, especially wiretaps and "bugs," and the Fourth Amendment implications of the government's use of these devices in the course of its investigations, the relevant statutes (and related Department of Justice guidelines) provide restrictions on the use of most electronic surveillance, including the requirement that a high-level Department official specifically approve the use of many of these types of electronic surveillance prior to an Assistant United States Attorney obtaining a court order authorizing interception.

Chapter 7 contains the specific mechanisms, including applicable approval requirements, for the use of wiretaps, "bugs" (oral interception devices), roving taps, video surveillance, and the consensual monitoring of wire or oral communications, as well as emergency interception procedures and restrictions on the disclosure and evidentiary use of information obtained through electronic surveillance. Additional information concerning use of the various types of electronic surveillance is also set forth in the Criminal Resource Manual at 27.

Attorneys in the Electronic Surveillance Unit of the Office of Enforcement Operations, Criminal Division, are available to provide assistance concerning both the interpretation of Title III and the review process necessitated thereunder. Interceptions conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, which is codified at 50 U.S.C. § 1801, *et seq.*, are specifically excluded from the coverage of Title III. *See* 18 U.S.C. § 2511(2)(a)(ii), (2)(e), and (2)(f).

9-7.100 Authorization of Applications for Wire, Oral, and Electronic Interception Orders -- Overview and History of Legislation

To understand the core concepts of the legislative scheme of Title III, one must appreciate the history of this legislation and the goals of Congress in enacting this comprehensive law. By enacting Title III in 1968, Congress prohibited private citizens from using certain electronic surveillance techniques. Congress exempted law enforcement from this prohibition, but required compliance with explicit directives that controlled the circumstances under which law enforcement's use of electronic surveillance would be permitted. Many of the restrictions upon the use of electronic surveillance by law enforcement agents were enacted in recognition of the

strictures against unlawful searches and seizures contained in the Fourth Amendment to the United States Constitution. *See, e.g., Katz v. United States*, 389 U.S. 347 (1967). Still, several of Title III's provisions are more restrictive than what is required by the Fourth Amendment. At the same time, Congress preempted State law in this area, and mandated that States that sought to enact electronic surveillance laws would have to make their laws at least as restrictive as the Federal law.

One of Title III's most restrictive provisions is the requirement that Federal investigative agencies submit requests for the use of certain types of electronic surveillance (primarily the non-consensual interception of wire and oral communications) to the Department of Justice for review and approval before applications for such interception may be submitted to a court of competent jurisdiction for an order authorizing the interception. Specifically, in 18 U.S.C. § 2516(1), Title III explicitly assigns such review and approval powers to the Attorney General, but allows the Attorney General to delegate this review and approval authority to a limited number of high-level Justice Department officials, including Deputy Assistant Attorneys General for the Criminal Division ("DAAGs"). The DAAGs review and approve or deny proposed applications to conduct "wiretaps" (to intercept wire [telephone] communications, 18 U.S.C. § 2510(1)) and to install and monitor "bugs" (the use of microphones to intercept oral [face-to-face] communications, 18 U.S.C. § 2510(2)). It should be noted that only those crimes enumerated in 18 U.S.C. § 2516(1) may be investigated through the interception of wire or oral communications. On those rare occasions when the government seeks to intercept oral or wire communications within premises or over a facility that cannot be identified with any particularity, and a "roving" interception of wire or oral communications is therefore being requested, the Assistant Attorney General or the Acting Assistant Attorney General for the Criminal Division must be the one to review and approve or deny the application. (See the roving interception provision at 18 U.S.C. § 2518(11), discussed at USAM 9-7.111.)

In 1986, Congress amended Title III by enacting the Electronic Communications Privacy Act of 1986. Specifically, Congress added a new category of covered communications, i.e., "electronic communications," which would now be protected, and whose interception would be regulated, by Title III. Electronic communications are those types of non-oral or wire communications that occur, *inter alia*, over computers, digital-display pagers, and facsimile ("fax") machines. *See* 18 U.S.C. § 2510(12).

Although the 1986 amendments permit any government attorney to authorize the making of an application to a Federal court to intercept electronic communications to investigate any Federal felony (18 U.S.C. § 2516(3)), the Department of Justice and Congress agreed informally at the time of ECPA's enactment that, for a three-year period, Department approval would nonetheless be required before applications could be submitted to a court to conduct interceptions of electronic communications. After that period, the Department rescinded the prior approval requirement for the interception of electronic communications over digital-display paging devices, but continued the need for Department approval prior to application to the court for the interception of electronic communications over any other device, such as computers and fax machines. Applications to the court for authorization to intercept electronic communications over digital-display pagers--which are the most commonly targeted type of electronic

communications--may be made based solely upon the authorization of a United States Attorney. *See* 18 U.S.C. § 2516(3).

Because there are severe penalties for the improper and/or unlawful use and disclosure of electronic surveillance evidence, including criminal, civil, and administrative sanctions, as well as the suppression of evidence, it is essential that Federal prosecutors and law enforcement agents clearly understand when Departmental review and approval are required, and what such a process entails. *See* 18 U.S.C. §§ 2511, 2515, 2518(10), and 2520.
See the Criminal Resource Manual at 31 for citations to relevant legislation.

9-7.110 Format for the Authorization Request

When Justice Department review and approval of a proposed application for electronic surveillance is required, the Electronic Surveillance Unit of the Criminal Division's Office of Enforcement Operations will conduct the initial review of the necessary pleadings, which include:

A. The affidavit of an "investigative or law enforcement officer" of the United States who is empowered by law to conduct investigations of, or to make arrests for, offenses enumerated in 18 U.S.C. § 2516(1) or (3) (which, for any application involving the interception of electronic communications, includes any Federal felony offense), with such affidavit setting forth the facts of the investigation that establish the basis for those probable cause (and other) statements required by Title III to be included in the application;

B. The application by any United States Attorney or his/her Assistant, or any other attorney authorized by law to prosecute or participate in the prosecution of offenses enumerated in 18 U.S.C. § 2516(1) or (3) that provides the basis for the court's jurisdiction to sign an order authorizing the requested interception of wire, oral, and/or electronic communications; and

C. A set of orders to be signed by the court authorizing the government to intercept, or approving the interception of, the wire, oral, and/or electronic communications that are the subject of the application, including appropriate redacted orders to be served on any relevant providers of "electronic communication service" (as defined in 18 U.S.C. § 2510(15)).

9-7.111 Roving Interception

Pursuant to 18 U.S.C. § 2518(11)(a) and (b), the government may obtain authorization to intercept wire, oral, and electronic communications of specifically named subjects without specifying with particularity the premises within, or the facilities over which, the communications will be intercepted. (Such authorization is commonly referred to as "roving" authorization.) As to the interception of oral communications, the government may seek authorization without specifying the location(s) of the interception when it can be shown that it is not practical to do so. *See United States v. Bianco*, 998 F.2d 1112 (2d Cir. 1993), *cert. denied*, 114 S. Ct. 1644 (1994); *United States v. Orena*, 883 F. Supp. 849 (E.D.N.Y. 1995). An application for the interception of wire and electronic communications of specifically named subjects may be made without specifying the facility or facilities over which the communications

will be intercepted when it can be shown that the subject or subjects of the interception have demonstrated a purpose to thwart interception by changing facilities. *See United States v. Gaytan*, 74 F.3d 545 (5th Cir. 1996); *United States v. Petti*, 973 F.2d 1441 (9th Cir. 1992), *cert. denied*, 113 S.Ct. 1859 (1993); *United States v. Villegas*, 1993 WL 535013 (S.D.N.Y. December 22, 1993).

When the government seeks authorization for roving interception, the Department's authorization must be made by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an Acting Assistant Attorney General. *See* 18 U.S.C. § 2518(11)(a)(i) and (b)(i).

9-7.112 Emergency Interception

Title III contains a provision which allows for the warrantless, emergency interception of wire, oral, and/or electronic communications. Specifically, under 18 U.S.C. § 2518(7), the Attorney General (AG), the Deputy Attorney General (DAG), or the Associate Attorney General (AssocAG) may specially designate a law enforcement or investigative officer to determine whether an emergency situation exists that requires the interception of wire, oral, and/or electronic communications before a court order authorizing such interception can, with due diligence, be obtained. As defined by 18 U.S.C. § 2518(7), an emergency situation involves either: (1) immediate danger of death or serious bodily injury to any person; (2) conspiratorial activities threatening the national security interest; or (3) conspiratorial activities characteristic of organized crime. The only situations which will likely constitute an emergency are those involving an imminent threat to life, i.e., a kidnapping or hostage taking. *See United States v. Crouch*, 666 F. Supp. 1414 (N.D. Cal. 1987)(wiretap evidence suppressed because there was no imminent threat of death or serious injury); *Nabozny v. Marshall*, 781 F.2d 83 (6th Cir.)(kidnapping and extortion scenario constituted an emergency situation), *cert. denied*, 476 U.S. 1161 (1986). The emergency provision also requires that grounds must exist under which an order could be entered (*viz.*, probable cause, necessity, specificity of target location/facility) to authorize the interception. Once the AG, the DAG, or the AssocAG authorizes the law enforcement agency to proceed with the emergency Title III, the government then has forty-eight (48) hours, from the time the authorization was granted, to obtain a court order approving the emergency interception. 18 U.S.C. § 2518(7). The affidavit supporting the application for the order must contain only those facts known to the AG, the DAG, or the AssocAG at the time his or her approval was given, and must be accompanied by a written verification from the requesting agency noting the date and time of the authorization. Failure to obtain the court order within the forty-eight-hour period will render any interceptions obtained during the emergency illegal.

Prior to the agency's contact with the AG, the DAG, or the Associate AG, oral approval to make the request must first be obtained from the Assistant Attorney General (AAG) or a Deputy Assistant Attorney General (DAAG) of the Criminal Division. This approval is facilitated by the Office of Enforcement Operation's Electronic Surveillance Unit, which is the initial contact for the requesting United States Attorney's Office and the requesting agency. Once the Electronic Surveillance Unit attorney briefs and obtains oral approval from the AAG or the DAAG, the attorney notifies the agency representative and the Assistant United States Attorney that the

Criminal Division recommends that the emergency authorization proceed. The agency then contacts the AG, the DAG, or the AssocAG and seeks permission to proceed with the emergency Title III.

9-7.200 Video Surveillance -- Closed Circuit Television -- Department of Justice Approval Required When There Is A Reasonable Expectation of Privacy

[redacted by WCS]

9-7.250 Use and Unsealing of Title III Affidavits

When the government terminates a Title III electronic surveillance investigation, it must maintain under seal all of the Title III applications and orders (including affidavits and accompanying material) that were filed in support of the electronic surveillance. *See* 18 U.S.C. § 2518(8)(b); *In re Grand Jury Proceedings*, 841 F.2d 1048, 1053 n.9 (11th Cir. 1988) (although 18 U.S.C. § 2518(8)(b) refers only to "applications" and "orders," "applications" is construed to include affidavits and any other related documentation).

The purpose of this sealing requirement is to ensure the integrity of the Title III materials and to protect the privacy rights of those individuals implicated in the Title III investigation. *See* S.Rep. No. 1097, *reprinted in* 1968 U.S. Code Cong. & Admin. News 2112, 2193-2194. The applications may be unsealed only pursuant to a court order and only upon a showing of good cause under 18 U.S.C. § 2518(8)(b) or in the interest of justice under 18 U.S.C. § 2518(8)(d).

Thus, the government attorney should not attach Title III affidavits or other application material as exhibits to any search warrant affidavit, complaint, indictment, or trial brief. The government attorney may, nevertheless, use information from these materials or the Title III interceptions in documents such as search warrant affidavits, complaints, indictments, and trial briefs. *See* 18 U.S.C. § 2517(8)(a); 18 U.S.C. § 2517(1) and (2); and S.Rep. No. 1097 at 2188. In using this information, however, the government attorney must use care not to disclose publicly information from the Title III affidavits or interceptions that would either abridge the privacy interests of persons not charged with any crime or jeopardize ongoing investigations.

When Title III materials are sought by defense counsel or other persons and the privacy interests of uncharged persons are implicated by the contents of those materials, the government attorney should seek a protective order pursuant to Rule 16(d)(1), Fed. R. Crim. P., that will forbid public disclosure of the contents of the materials. Likewise, a Rule 16 protective order should be sought to deny or defer discovery of those portions of the affidavits and applications that reveal ongoing investigations when disclosure would jeopardize the success of any such investigation.
For discussion about disclosure of intercepted communications in civil litigation see the Criminal Resource Manual at 33-34.

9-7.301 Consensual Monitoring -- General Use

Section 2511(2)(c) of Title 18 provides that "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...." *See United States v. White*, 401 U.S. 745 (1971). As such, consensual interceptions need not be made under Title III procedures, interception orders under § 2518 are not available, and should not be sought in cases falling within § 2511(2)(c).

[redacted by WCS]

II. NEED FOR WRITTEN AUTHORIZATION

A. Investigations Where Written Department of Justice Approval is Required. A request for authorization to monitor an oral communication without the consent of all parties to the communication must be approved in writing by the Director or Associate Directors of the Office of Enforcement Operations, Criminal Division, U.S. Department of Justice, when it is known that:

(1) the monitoring relates to an investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years;

(2) the monitoring relates to an investigation of the Governor, Lieutenant Governor, or Attorney General of any State or Territory, or a judge or justice of the highest court of any State or Territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his or her official duties;

(3) any party to the communication is a member of the diplomatic corps of a foreign country;

(4) any party to the communication is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers;

(5) the consenting or nonconsenting person is in the custody of the Bureau of Prisons or the United States Marshals Service; or

(6) the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or the United States Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent before conducting consensual monitoring in a specific investigation.

In all other cases, approval of consensual monitoring will be in accordance with the procedures set forth in part V. below.

B. Monitoring Not Within Scope of Memorandum. Even if the interception falls within one of the six categories above, the procedures and rules in this Memorandum do not apply to:

(1) extraterritorial interceptions;

(2) foreign intelligence interceptions, including interceptions pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. §1801, *et seq*.);

(3) interceptions pursuant to the court-authorization procedures of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (18 U.S.C. §2510, *et seq*.);

(4) routine Bureau of Prisons monitoring of oral communications that are not attended by a justifiable expectation of privacy;

(5) interceptions of radio communications; and

(6) interceptions of telephone communications.

III. AUTHORIZATION PROCEDURES AND RULES
[redacted by WCS]

9-7.400 Defendant Motion or Discovery Request for Disclosure of Defendant Overhearings and Attorney Overhearings

[redacted by WCS]

9-7.500 Prior Consultation with the Computer Crime and Intellectual Property Section of the Criminal Division (CCIPS) for Applications for Pen Register and Trap and Trace Orders Capable of Collecting Uniform Resource Locators (URLs)

[redacted by WCS]

Criminal Resource Manual:

Electronic Surveillance -- Title III Applications

The Application should meet the following requirements:

A. It must be prepared by an applicant identified as a law enforcement or investigative officer. The application must be in writing, signed by the United States Attorney, an Assistant United States Attorney, and made under oath. It must be presented to a Federal district court or court of appeals judge and be accompanied by the Department's authorization memorandum signed by an appropriate Department of Justice official. **The application may not be presented to a magistrate**. *See* 18 U.S.C. §§ 2510(9) and 2516(1); *see also In re United States of America*, 10 F.3d 931 (2d Cir. 1993), *cert. denied*, 115 S. Ct. 64 (1994).
B. It must identify the type of communications to be intercepted. "Wire communications" include "aural transfers" (involving the human voice) that are

transmitted, at least in part by wire, between the point of origin and the point of reception, i.e., telephone calls. 18 U.S.C. § 2510(1). This includes cellular phones, cordless phones, voice mail, and voice pagers, as well as traditional landline telephones. "Oral communications" are communications between people who are together under circumstances where the parties enjoy a reasonable expectation of privacy. 18 U.S.C. § 2510(2). An "electronic communication" most commonly involves digital-display paging devices or fax machines, but also includes electronic mail, computer transmissions, and, in some cases, satellite transmissions. It does not include tone-only paging devices, tracking devices (as defined by 18 U.S.C. 3117), or electronic funds transfer information. 18 U.S.C. § 2510(12).

C. It must identify the specific Federal offenses for which there is probable cause to believe are being committed. The offenses that may be the predicate for a wire or oral interception order are limited to only those set forth in 18 U.S.C. § 2516(1). In the case of electronic communications, a request for interception may be based on any Federal felony, pursuant to 18 U.S.C. § 2516(3).

D. It must provide a particular description of the nature and location of the facilities from which, or the place where, the interception is to occur. An exception to this is the roving interception provision set forth in 18 U.S.C. § 2518(11)(a) and (b). The specific requirements of the roving provision are discussed in USAM 9-7.111. Briefly, in the case of a roving oral interception, the application must show, and the court order must indicate, that it is impractical to specify the location(s) where oral communications of a particular named subject are to be intercepted. 18 U.S.C. § 2518(11)(a)(ii) and (iii). In the case of a roving wire or electronic interception, the application must state, and the court order must indicate, that a particular named subject is using various and changing facilities for the purpose of thwarting electronic surveillance. 18 U.S.C. § 2518(11)(b)(ii) and (iii). The accompanying DOJ document authorizing the roving interception must be signed by an official at the level of an Assistant Attorney General (including Acting AAG) or higher. 18 U.S.C. § 2518(11)(a)(i) and (b)(i).

E. It must identify, with specificity, those persons known to be committing the offenses and whose communications are to be intercepted. In *United States v. Donovan*, 429 U.S. 413 (1977), the Supreme Court stated that 18 U.S.C. § 2518(1)(b)(iv) requires the government to name all individuals whom it has probable cause to believe are engaged in the offenses under investigation, and whose conversations it expects to intercept over or from within the targeted facilities. It is the Department's policy to name as potential subjects all persons whose involvement in the alleged offenses is indicated. *See United States v. Ambrosio*, 898 F. Supp. 177 (S.D.N.Y. 1995); *United States v. Marcy*, 777 F. Supp. 1400 (N.D. Ill. 1991); *United States v. Martin*, 599 F.2d 880 (9th Cir.), *cert. denied*, 441 U.S. 962 (1979).

F. It must contain a statement affirming that normal investigative procedures have been tried and failed, are reasonably unlikely to succeed if tried, or are too dangerous to employ. 18 U.S.C. § 2518(1)(c). The applicant may then state that a complete discussion of attempted alternative investigative techniques is set forth in the accompanying affidavit.

G. It must contain a statement affirming that the affidavit contains a complete statement of the facts--to the extent known to the applicant and the official approving the application--concerning all previous applications that have been made to intercept the oral, wire, or electronic communications of any of the named subjects or involving the target facility or location. 18 U.S.C. § 2518(1)(e).
H. In an oral (and occasionally in a wire or electronic) interception, it must contain a request that the court issue an order authorizing investigative agents to make all necessary surreptitious and/or forcible entries to install, maintain, and remove electronic interception devices in or from the targeted premises (or device). When effecting this portion of the order, the applicant should notify the court as soon as practicable after each surreptitious entry.
I. It should, when requesting the interception of wire communications, contain a request that the authorization and court order apply not only to the target telephone number(s) identified therein, but to any changed telephone number(s) subsequently assigned to the same cable, pair, and binding posts used by each targeted landline telephone. With regard to a cellular telephone, the request should be that the authorization and order apply not only to any identified telephone number, but also to any changed telephone number or any other telephone subsequently assigned to the instrument bearing the same electronic serial number as the targeted cellular phone. The application should also request that the authorization apply to background conversations intercepted in the vicinity of the target phone while the phone is off the hook or otherwise in use. *See United States v. Baranek*, 903 F.2d 1068 (6th Cir. 1990).
J. It must contain, when concerning the interception of wire communications, a request that the court issue an order directly to the service provider, as defined in 18 U.S.C. § 2510(15), to furnish the investigative agency with all information, facilities, and technical assistance necessary to facilitate the ordered interception. 18 U.S.C. § 2511(2)(a)(ii). The application should also request that the court direct service providers and their agents and employees not to disclose the contents of the court order or the existence of the investigation. *Id.*
K. It should contain a request that the court's order authorize the requested interception until all relevant communications have been intercepted, not to exceed a period of thirty (30) days from the earlier of the day on which the interception begins or ten (10) days after the order is entered. 18 U.S.C. § 2518(5).
L. It should contain a statement affirming that all interceptions will be minimized in accordance with Chapter 119 of Title 18, United States Code, as described further in the affidavit. 18 U.S.C. § 2518(5).

Electronic Surveillance -- Title III Affidavits

The Affidavit must meet the following requirements:

A. It must be sworn and attested to by an investigative or law enforcement officer as defined in 18 U.S.C. § 2510(7). Department policy precludes the use of multiple

affiants except when it is indicated clearly which affiant swears to which part of the affidavit, or states that each affiant swears to the entire affidavit. If a State or local law enforcement officer is the affiant in a Federal electronic surveillance affidavit, the enforcement officer must be *deputized* as a Federal officer of the agency responsible for the offenses under investigation. 18 U.S.C. § 2516(1).

B. It must identify those persons who will be the focus of the surveillance, describe the facility or location that is the subject of the proposed electronic surveillance, and list the alleged offenses. 18 U.S.C. § 2518(1).

C. It must establish probable cause that the named subjects are using the targeted facility or location to commit the stated offenses. (When the application requests authorization to intercept oral communications within a location, the FBI requires that a diagram of the target location be submitted as an attachment to the affidavit.) Any background information needed to understand fully the instant investigation should be set forth briefly at the beginning of this section. The focus, however, should be on recent and current criminal activity by the subjects, with an emphasis on their use of the target facility or location. This is generally accomplished through information from a confidential informant, cooperating witness, or undercover agent, combined with pen register or telephone toll information for the target phone or physical surveillance of the target premises. It is Department of Justice policy that pen register or telephone toll information for the target telephone, or physical surveillance of the targeted premises, standing alone, is generally insufficient to establish probable cause. Probable cause to establish criminal use of the facilities or premises requires independent evidence of use of the facilities or premises in addition to pen register or surveillance information (e.g., informant or undercover information.) It is preferable that all informants used in the affidavit to establish probable cause be qualified according to the "Aguilar-Spinelli" standards (*Aguilar v. Texas*, 378 U.S. 108 (1964) and *Spinelli v. United States*, 393 U.S. 410 (1969)), rather than those set forth in the Supreme Court decision of *Illinois v. Gates*, 463 U.S. 1237 (1983). On rare occasions, criminal use of the target facilities or premises may be established solely by an extremely high volume of calls to, or meetings with, other known or suspected co-conspirators that coincide with incidents of known illegal activity. It is also the Department's policy that the affidavit reflect use of the target facility or premises within twenty-one days of the date on which the Department authorizes the filing of the application. While the subjects' use of the target facilities or premises may be updated to within twenty-one days through pen register information and/or physical surveillance, historical information (*viz*., information older than six months from the date of the application), combined with pen register information or physical surveillance alone, is generally insufficient to establish probable cause under existing Department policy.

D. It must explain the need for the proposed electronic surveillance and provide a detailed discussion of the other investigative procedures that have been tried and failed, are reasonably unlikely to succeed if tried, or are too dangerous to employ. 18 U.S.C. § 2518(1)(e). This is to ensure that highly intrusive electronic surveillance techniques are not resorted to in situations where traditional investigative techniques would suffice to expose the crime. *United States v. Kahn*,

415 U.S. 143 (1974). It need not be shown that no other investigative avenues are available, only that they have been tried and proven inadequate or have been considered and rejected for reasons described. *See United States v. Castillo-Garcia*, 920 F. Supp. 1537 (D. Colo. 1996); *United States v. Oriakhi*, 57 F.3d 1290 (4th Cir. 1995); *United States v. Torres*, 901 F.2d 205 (2d Cir.), *cert. denied*, 498 U.S. 906 (1990); *United States v. Clerkley*, 556 F.2d 709 (4th Cir. 1977). There should also be a discussion as to why electronic surveillance is the technique most likely to succeed. When drafting this section of the affidavit, the discussion of these and other investigative techniques should be augmented with facts particular to the specific investigation and subjects. General declarations and conclusory statements about the exhaustion of alternative techniques will not suffice.

It is most important that this section be tailored to the facts of the specific case and be more than a recitation of "boiler plate." The affidavit must discuss the particular problems involved in the investigation in order to fulfill the requirement of 18 U.S.C. § 2518(1)(c). The affidavit should explain specifically why other normally utilized investigative techniques, such as physical surveillance or the use of informants and undercover agents, are inadequate in the particular case. For example, if physical surveillance is impossible or unproductive because the suspects live in remote areas or will likely be alerted to law enforcement presence (by counter-surveillance or other means), the affidavit should set forth those facts clearly. If the informants refuse to testify or cannot penetrate the hierarchy of the criminal organization involved, the affidavit should explain why that is so in this particular investigation. If undercover agents cannot be used because the suspects deal only with trusted associates/family, the affidavit must so state and include the particulars. Conclusory generalizations about the difficulties of using a particular investigative technique will not suffice. It is not enough, for example, to state that the use of undercover agents is always difficult in organized crime cases because crime families, in general, deal only with trusted associates. While the affidavit may contain a general statement regarding the impossibility of using undercover agents in organized crime cases, it must also demonstrate that the particular subject or subjects in the instant case deal only with known associates. The key is to tie the inadequacy of a specific investigative technique to the particular facts underlying the investigation. *See, e.g.*, *United States v. Uribe*, 890 F.2d 554 (1st Cir. 1989); *United States v. Ashley*, 876 F.2d 1069 (1st Cir. 1989); *United States v. Zambrana*, 841 F.2d 1320 (7th Cir. 1988); and *United States v. Kalustian*, 529 F.2d 585 (9th Cir. 1976).

E. It must contain a full and complete statement of any prior electronic surveillance involving the persons, facilities, or locations specified in the application. This statement should also include the date, jurisdiction, and disposition of previous applications, as well as their relevance, if any, to the instant investigation. The duty to disclose prior applications under 18 U.S.C. § 2518(1)(e) covers all persons named in the application, and not just those designated as "principal targets." *United States v. Bianco*, 998 F.2d 1112 (2d Cir. 1993), *cert. denied*, 114 S. Ct. 1644 (1994). In addition to any known prior applications, the agency conducting the investigation should run a check of its electronic surveillance indices. In narcotics investigations, it is the Criminal Division's policy that both the DEA and the FBI conduct an indices check. In joint

investigations, all participating agencies should be checked; in all other cases when it is likely that more than one agency may have investigated the subjects, multiple indices checks should likewise be made.

F. It must contain a statement of the period of time for which the interception is to be maintained. The statute provides that an order may be granted for not more than thirty days or until the objectives of the investigation are achieved, whichever occurs first. 18 U.S.C. § 2518(5). If the violations are continuing, facts sufficient to justify interception for the full thirty-day period must be provided, or the court may order monitoring to cease once initial, criminal conversations are intercepted. This may be accomplished by showing, through informant or undercover investigation, pen register analysis, physical surveillance or other law enforcement investigation, that a pattern of criminal activity exists and is likely to continue. If it is clear that the interceptions will terminate after a limited number of days, then the time requested should also be so limited in accordance with the facts of the case.

   The statute also provides for a ten-day grace period, intended primarily for the installation of oral monitoring equipment, before the thirty-day period begins to be calculated. This provision may also be used when delays arise in installing monitoring devices used in wire or electronic interceptions. 18 U.S.C. § 2518(5). In either case, the provision is not intended to provide for a regular additional ten-day start-up period; any delays that are encountered should be real and defensible if challenged. The ten-day grace period applies only to the *initial* installation of equipment, and should not be used in an extension application, in an original application when the equipment is already installed, or in wire interception cases when a pen register permitting almost immediate access is already in place on the target phone. 18 U.S.C. § 2518(5). Under Rule 45 of the Federal Rules of Criminal Procedure, the thirty-day time period would begin to run on the date after the order was signed, even if the interception started on the same day it was signed. *See also United States v. Villegas*, 1993 WL 535013 (S.D.N.Y. December 22, 1993)(unreported); *United States v. Gerena*, 695 F. Supp. 649 (D. Conn. 1988). In an abundance of caution, however, the Department recommends that the thirty-day period be calculated from the date and time that the order is signed. This is particularly so when no delays are encountered which would permit the government to invoke the ten-day grace period allowed by the statute.

G. It must contain a statement affirming that monitoring agents will minimize all non-pertinent interceptions in accordance with Chapter 119 of Title 18, United States Code, as well as additional standard minimization language and other language addressing any specific minimization problems (e.g., steps to be taken to avoid the interception of privileged communications, such as attorney-client communications) in the instant case. (18 U.S.C. § 2518(5) permits non-officer government personnel or individuals acting under contract with the government to monitor conversations pursuant to the interception order. These individuals must be acting under the supervision of an investigative or law enforcement officer when monitoring communications, and the affidavit should note the fact that these individuals will be used as monitors pursuant to 18 U.S.C. § 2518(5).)

   When communications are intercepted that relate to any offense not enumerated in the authorization order, the monitoring agent should report it immediately to the Assistant United States Attorney, who should notify the court at the earliest opportunity. Approval by the issuing judge should be sought for the continued interception of such conversations. While 18 U.S.C. §§

2517(1) and (2) permit use or disclosure of this information without first obtaining a court order, 18 U.S.C. § 2517(5) requires a disclosure order before the information may be used in any proceeding (e.g., before a grand jury).

The statute permits after-the-fact minimization for wire and oral communications when the intercepted communications are in code, or in a foreign language when a foreign language expert is not *reasonably* available. 18 U.S.C. § 2518(5). In either event, the minimization must be accomplished as soon as practicable after the interception. Such after-the-fact minimization can be accomplished by an interpreter who listens to and minimizes the communications after they have been recorded, giving only the pertinent communications to the supervising agent. The process utilized must protect the suspect's privacy interests to approximately the same extent as would contemporaneous minimization, properly applied. *United States v. David*, 940 F.2d 722 (1st Cir.), *cert. denied*, 502 U.S. 989 (1991); *United States v. Gambino*, 734 F. Supp. 1084 (S.D.N.Y. 1990). After-the-fact minimization provisions should be applied in light of the "reasonableness" standard established by the Supreme Court in *United States v. Scott*, 436 U.S. 128 (1978).

After-the-fact minimization is a necessity for the interception of electronic communications over a digital-display pager or a fax machine. In such cases, all communications are recorded and then examined by a monitoring agent and/or a supervising attorney to determine their relevance to the investigation. Disclosure is then limited to those communications by the subjects or their confederates that are criminal in nature. *See United States v. Tutino*, 883 F.2d 1125 (2d Cir. 1989), *cert. denied*, 493 U.S. 1081 (1990).

H. When the request is to tap a cellular telephone or other portable telephone, or a portable paging device, or to install a bug in an automobile, the affidavit should contain a statement that, pursuant to 18 U.S.C. § 2518(3), interception will occur not only within the territorial jurisdiction of the court in which the application is made, but also outside that jurisdiction (but within the United States), if there is any indication that the target telephone, paging device or vehicle will be taken outside the jurisdiction of the court issuing the electronic surveillance order. The order should authorize such extra-jurisdictional interception, and such order should be sought in the jurisdiction having the strongest investigative nexus to the object in which the monitoring device is installed.

Electronic Surveillance -- Title III Orders

The Order must meet the following requirements:

The authorizing language of the order should mirror the requesting language of the application and affidavit, stating that there is probable cause to believe that the named subjects are committing particular Title III predicate offenses (or, in the case of electronic communications, any Federal felony), that they are using the target facility or premises in furtherance thereof, and that normal investigative techniques have been tried and have failed, or are reasonably unlikely to succeed if tried, or are too dangerous to employ. 18 U.S.C. § 2518(3) and (4). The court then orders (again tracking the language of the application and affidavit) that agents of the

investigative agency are authorized to intercept wire, oral, or electronic communications over the described facility or at the described premises. *Id.* The order should also contain language specifying the length of time the interception may be conducted, and, if necessary, authorizing surreptitious and/or forcible entry to effectuate the purpose of the order. *Id.* The order may also contain language mandating the government to make periodic progress reports (pursuant to 18 U.S.C. § 2518(6)), and ordering the sealing of these as well as the order, application and affidavit. In the case of a roving interception, the court must make a specific finding that the requirements of 18 U.S.C. § 2518(11)(a) and/or (b) have been demonstrated adequately. Any other special requests, such as extra-jurisdictional interception in the case of mobile interception devices, should also be authorized specifically in the order.

The court should also issue a technical assistance order to the communications service provider. 18 U.S.C. § 2518(4). This is a redacted order that requires the telephone company or other service provider to assist the agents in effecting the electronic surveillance. An order to seal all of the pleadings should also be sought at this time.

The above pleadings should be transmitted by the most expeditious means possible to the Office of Enforcement Operations, either by fax, directed to (202) 616-2010 or (202) 616-2038, or by Federal Express or other Department-approved carrier, addressed to the Office of Enforcement Operations' Electronic Surveillance Unit, Suite 900 West, 1001 G. Street, N.W, Washington, D.C. 20001. Prior to mailing, OEO should be contacted at (202) 514-6809 and advised that the material is forthcoming, as well as any special time considerations. Note that it is a violation of Department security regulations to transmit the sensitive information in electronic surveillance requests via E-mail.

It should also be noted that OEO cannot forward a request for authorization to an appropriate Department official for review and approval unless and until a formal, written request for authorization is received from the head of the investigative agency that will be conducting the investigation. Because of the time normally necessary for the Federal investigative agencies to complete their internal review and recommendation process, at least one week should be allowed for such process. The Assistant United States Attorney should ensure that the investigator has contacted his/her agency's headquarters in Washington, D.C., as far in advance as possible so that any problems with the pleadings or the underlying investigation can be resolved as expeditiously as possible.

Spinoff requests (*viz.*, additional applications to conduct electronic surveillance at a new location or over a new facility) are considered original applications and are reviewed in the same manner as described above. Extension requests still need Department approval, but only require review by OEO, and not the investigative agency. While the exigencies of investigative work occasionally make the normally required lead time impossible, the timeliness with which an application is reviewed and authorized is largely under the control of the Assistant United States Attorney handling the case. When coordinating an investigation or planning extension requests, it is important to allow sufficient time for the Title III application to be reviewed by both OEO and, if appropriate, the investigative agency.

Electronic Surveillance -- Statutory Authority and Legislative History

The Federal electronic surveillance statutes (commonly referred to collectively as "Title III") were originally enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub.L. 90-351, 82 Stat. 197 (June 19, 1968)("Title III"), and they have been substantially amended and updated as part of the Electronic Communications Privacy Act of 1986, Pub.L. 99-508, 100 Stat. 1848 (October 21, 1986)("ECPA"), the Communications Assistance for Law Enforcement Act, Pub.L. 103-414, 108 Stat. 4279 (October 24, 1994)("CALEA"), and the Antiterrorism and Effective Death Penalty Act of 1996, Pub.L. 104-132, 110 Stat. 1214 (April 24, 1996)("Antiterrorism Act"). These statutes are codified, *inter alia*, at 18 U.S.C. § 2510, *et seq*.

A partial legislative history for Title III, ECPA, CALEA, and the Antiterrorism Act may be found in, respectively: S.Rep. No. 1097, 90th Cong., 2d Sess. (1968), *reprinted in* 1968 U.S. Code Cong. & Admin. News ("U.S.C.C.A.N.") 2112 (Title III); S.Rep. No. 541, 99th Cong., 2d Sess. (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555 (ECPA); S.Rep. No. 402, 103d Cong., 2d Sess. (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489 (CALEA); and H.R. Rep. No. 518, 104th Cong., 2d Sess. (1996), *reprinted in* ____ U.S.C.C.A.N. ____ (Antiterrorism Act).