



[Email this Document!](#)

**UNITED STATES CODE ANNOTATED**  
**TITLE 18. CRIMES AND CRIMINAL PROCEDURE**  
**PART I--CRIMES**  
**CHAPTER 119--WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND**  
**INTERCEPTION OF ORAL COMMUNICATIONS**

---

**§ 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.

### **§ 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 signed by the authorizing judge, or

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

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

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

[(c) Redesignated (b)]

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

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

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

then the person who engages in such conduct shall be subject to suit by the Federal Government in a

court of competent jurisdiction.

(ii) In an action under this subsection--

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

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

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

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

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

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

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

(c) places in any newspaper, magazine, handbill, or other publication 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.

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

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

**§ 2515. Prohibition of use as evidence of intercepted wire or oral communications**

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

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

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

(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 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 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (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 1014 (relating to loans and credit applications generally; renewals and discounts), 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), 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 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 1992 (relating to wrecking trains), 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);

**(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) or section 46502 (relating to aircraft piracy) 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) of this title or a violation of section 274, 277, or 278 of the Immigration and Nationality Act (relating to the smuggling of aliens);

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

**(r)** 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.

**§ 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.

#### **§ 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.

**§ 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.

#### **§ 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).

### **§ 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.

### **§ 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.

- 
- [More Information on: Federal Statutes Related to Cybercrime generally](#)
  - [More Information on: Federal Statutes Related to Computer Intrusions](#)

Go To .. [CCIPS Home Page](#) || [Justice Department Home Page](#)

---

*Updated July 9, 2003*  
usdoj-crm/mis/krr

---



**UNITED STATES CODE ANNOTATED**  
**TITLE 18. CRIMES AND CRIMINAL PROCEDURE**  
**PART I--CRIMES**  
**CHAPTER 121--STORED WIRE AND ELECTRONIC COMMUNICATIONS AND**  
**TRANSACTIONAL**  
**RECORDS ACCESS**

---

**§ 2701. Unlawful access to stored communications**

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

- (1)** intentionally accesses without authorization a facility through which an electronic communication service is provided; or
- (2)** intentionally exceeds an authorization to access that facility;

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

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

**(1)** if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State--

**(A)** a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and

**(B)** a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

**(2)** in any other case--

**(A)** a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

**(B)** a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

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

- (1) by the person or entity providing a wire or electronic communications service;
- (2) by a user of that service with respect to a communication of or intended for that user; or
- (3) in section 2703, 2704 or 2518 of this title.

## § 2702. Voluntary disclosure of customer communications or records

### (a) Prohibitions.--Except as provided in subsection (b)--

- (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
- (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--
  - (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
  - (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and
- (3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

### (b) Exceptions for disclosure of communications.-- A provider described in subsection (a) may divulge the contents of a communication--

- (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
- (2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;
- (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
- (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;
- (5) as may be necessarily incident to the rendition of the service or to the protection of the

rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);

(7) to a law enforcement agency--

(A) if the contents--

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

(ii) appear to pertain to the commission of a crime; or

[(B) Repealed. Pub.L. 108-27, Title V, § 508(b)(1)(A), April 30, 2003, 117 Stat. 650]

[(C) Repealed. Pub.L. 107-296, Title II, § 225(d)(1)(C), Nov. 25, 2002, 116 Stat. 2157]

(8) to a Federal, State, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

**(c) Exceptions for disclosure of customer records.**--A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

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

(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032); or

(6) to any person other than a governmental entity.

### § 2703. Required disclosure of customer communications or records

**(a) Contents of wire or electronic communications in electronic storage.**--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

**(b) Contents of wire or electronic communications in a remote computing service.**--(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

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

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

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

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

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

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

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

**(c) Records concerning electronic communication service or remote computing service.**--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;

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

(C) has the consent of the subscriber or customer to such disclosure; or

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

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

**(d) Requirements for court order.**--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the



information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

**(e) No cause of action against a provider disclosing information under this chapter.**--No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

**(f) Requirement to preserve evidence.**--

**(1) In general.**--A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

**(2) Period of retention.**--Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90- day period upon a renewed request by the governmental entity.

**(g) Presence of officer not required.**--Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

#### **§ 2704. Backup preservation**

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

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

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

**(A)** the delivery of the information; or

**(B)** the resolution of any proceedings (including appeals of any proceeding)

concerning the government's subpoena or court order.

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

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

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

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

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

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

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

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

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

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

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

### § 2705. Delayed notice

(a) **Delay of notification.**--(1) A governmental entity acting under section 2703(b) of this title may--

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

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

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

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

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

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

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

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days

each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

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

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

(B) informs such customer or subscriber--

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

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

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

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

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

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

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

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

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

### § 2706. Cost reimbursement

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

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

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

### § 2707. Civil action

**(a) Cause of action.**--Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

**(b) Relief.**--In a civil action under this section, appropriate relief includes--

- (1) such preliminary and other equitable or declaratory relief as may be appropriate;
- (2) damages under subsection (c); and
- (3) a reasonable attorney's fee and other litigation costs reasonably incurred.

**(c) Damages.**--The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of \$1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability

under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

**(d) 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."

**(e) Defense.**--A good faith reliance on--3

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title);

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

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

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

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

**(g) Improper disclosure.**--Any willful disclosure of a 'record', as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.

### § 2708. Exclusivity of remedies

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

### § 2709. Counterintelligence access to telephone toll and transactional records

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

**(b) Required certification.**--The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may--

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

**(c) Prohibition of certain disclosure.**--No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

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

**(e) Requirement that certain congressional bodies be informed.**--On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

## § 2710. Wrongful disclosure of video tape rental or sale records

**(a) Definitions.**--For purposes of this section--

(1) the term "consumer" means any renter, purchaser, or subscriber of goods or services from a video tape service provider;

(2) the term "ordinary course of business" means only debt collection activities, order fulfillment, request processing, and the transfer of ownership;

(3) the term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider; and

(4) the term "video tape service provider" means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

**(b) Video tape rental and sale records.**--(1) A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).

(2) A video tape service provider may disclose personally identifiable information concerning any consumer--

(A) to the consumer;

(B) to any person with the informed, written consent of the consumer given at the time the disclosure is sought;

(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;

(D) to any person if the disclosure is solely of the names and addresses of consumers and if--

(i) the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and

(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;

(E) to any person if the disclosure is incident to the ordinary course of business of the video tape service provider; or

(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if--



(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.

If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the video tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

(c) **Civil action.**--(1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.

(2) The court may award--

(A) actual damages but not less than liquidated damages in an amount of \$2,500;

(B) punitive damages;

(C) reasonable attorneys' fees and other litigation costs reasonably incurred; and

(D) such other preliminary and equitable relief as the court determines to be appropriate.

(3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.

(4) No liability shall result from lawful disclosure permitted by this section.

(d) **Personally identifiable information.**--Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, 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 of a State.

(e) **Destruction of old records.**--A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for

access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order.

**(f) Preemption.**--The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.

### § 2711. Definitions for chapter

As used in this chapter--

- (1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;
- (2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system; and
- (3) the term "court of competent jurisdiction" has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.

### § 2712. Civil actions against the United States

**(a) In general.**--Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U. S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages--

- (1) actual damages, but not less than \$10,000, whichever amount is greater; and
- (2) litigation costs, reasonably incurred.

**(b) Procedures.**--(1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.

(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.

(3) Any action under this section shall be tried to the court without a jury.

(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et

seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

**(c) 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.

**(d) Exclusive remedy.**--Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

**(e) Stay of proceedings.**--(1) Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).

(2) In this subsection, the terms "related criminal case" and "related investigation" mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical.

(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party.

- 
- [More Information on: Federal Statutes Related to Cybercrime generally](#)
  - [More Information on: Federal Statutes Related to Computer Intrusions](#)
  - [More Information on: Changes Resulting from Sec. 896 of the 2002 Homeland Security Act and Sec. 225 of the 2002 Cyber Security Enhancement Act](#)

Go to . . . [CCIPS Home Page](#) || [Justice Department Home Page](#)

---

*Updated page May 19, 2003*

*usdoj-crm/mis/lrr*

---

LexisNexis® Total Research System Switch Client | Preferences | Sign Out | Help

My Lexis™ Search Research Tasks Get a Document Shepard's® Alerts Total Litigator Transactional Advisor Counsel Selector History

FOCUS™ Terms Search Within Original Results (1 - 34) Advanced...

Source: [Legal](#) > /.../ > [FL State Cases, Combined](#)

Terms: "o'brien v. o'brien" ([Edit Search](#) | [Suggest Terms for My Search](#))

Select for FOCUS™ or Delivery



899 So. 2d 1133, \*; 2005 Fla. App. LEXIS 1408, \*\*;  
30 Fla. L. Weekly D 430

BEVERLY ANN O'BRIEN, Appellant, v. JAMES KEVIN O'BRIEN, Appellee.

Case No. 5D03-3484

COURT OF APPEAL OF FLORIDA, FIFTH DISTRICT

899 So. 2d 1133; 2005 Fla. App. LEXIS 1408; 30 Fla. L. Weekly D 430

February 11, 2005, Opinion Filed

#### SUBSEQUENT HISTORY: [\*\*1]

Rehearing denied by [O'Brien v. O'Brien, 2005 Fla. App. LEXIS 6050 \(Fla. Dist. Ct. App. 5th Dist., Apr. 29, 2005\)](#)

**PRIOR HISTORY:** Appeal from the Circuit Court for Orange County, Donald E. Grincewicz, Judge.

**DISPOSITION:** AFFIRMED.

#### CASE SUMMARY

**PROCEDURAL POSTURE:** The Circuit Court for Orange County (Florida), without considering certain communications obtained surreptitiously from appellee husband's computer by appellant wife by the use of a spyware program, entered a final judgment of dissolution of marriage. The wife's motion for rehearing was denied. She appealed the trial court's order granting a permanent injunction, the final judgment, and the order denying her motion for rehearing.

**OVERVIEW:** The wife secretly installed a spyware program on the husband's computer. It was undisputed that the husband engaged in private on-line chats with another woman. The husband received a permanent injunction to prevent the wife's disclosure of the communications and to prevent her from engaging in that activity in the future. The trial court precluded introduction of the communications into evidence in the divorce proceeding. The wife argued that the electronic communications were retrieved from storage and, therefore, were not "intercepted communications" as defined by the Security of Communications Act. The appellate court held the clear intent of [Fla. Stat. ch. 934.03](#) (2003) was to make it illegal for a person to intercept wire, oral, or electronic communications. The communications were "electronic communications" which were intercepted contemporaneously with transmission. Thus, the electronic communications were intercepted in violation of the Act. While the intercepted electronic communications were not excludable under the Act, because the evidence was illegally obtained, the trial court did not abuse its discretion in refusing to admit it.

**OUTCOME:** The judgment of the trial court was affirmed.

**CORE TERMS:** electronic communications, intercepted, intercept, storage, interception, wire, spyware, Federal Wiretap Act, electronic, installed, endeavor, wire communication, conversation, transmission, transmitted, copied, stored, e-mails, retrieval, disclose, drive, illegally obtained, criminal investigation, oral communication, reason to know, contemporaneously, acquisition, software, message, privacy

#### LEXISNEXIS® HEADNOTES

[Hide](#)

[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Miscellaneous Offenses](#) > [Illegal Eavesdropping](#) > [Elements](#)

**HN2** See [Fla. Stat. ch. 934.03\(1\)](#) (2003).


[Communications Law](#) > [Federal Acts](#) > [Communications Act](#) > [General Overview](#)

[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Miscellaneous Offenses](#) > [Illegal Eavesdropping](#) > [General Overview](#)


**HN2** Enactment of the prohibitions in [Fla. Stat. ch. 934.03\(1\)](#) (2003) connotes a policy decision by the Florida Legislature to allow each party to a conversation to have an expectation of privacy from interception by another party to the conversation. The purpose of the Security of Communications Act is to protect every person's right to privacy and to prevent the pernicious effect on all citizens who would otherwise feel insecure from intrusion into their private conversations and communications. [More Like This Headnote](#)


[Computer & Internet Law](#) > [Criminal Offenses](#) > [Data Crimes & Fraud](#)

[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Fraud](#) > [Computer Fraud](#) > [General Overview](#)


[Evidence](#) > [Illegal Eavesdropping](#) > [General Overview](#) 

**HN3** The clear intent of the Florida Legislature in enacting [Fla. Stat. ch. 934.03](#) (2003) is to make it illegal for a person to intercept wire, oral, or electronic communications. [More Like This Headnote](#)


[Communications Law](#) > [Federal Acts](#) > [Communications Act](#) > [Penalties](#) 


[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Miscellaneous Offenses](#) > [Illegal Eavesdropping](#) > [Elements](#) 


**HN4** The term "intercept" is defined by the Security of Communications Act as 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. [Fla. Stat. ch. 934.02\(3\)](#) (2003). [More Like This Headnote](#) | [Shepardize: Restrict By Headnote](#)

[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Miscellaneous Offenses](#) > [Illegal Eavesdropping](#) > [General Overview](#) 


**HN5** The term "electronic communications" is defined in [Fla. Stat. ch. 934.02\(12\)](#) (2003) as any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects intrastate, inter-state, or foreign commerce. [More Like This Headnote](#)

[Computer & Internet Law](#) > [Privacy & Security](#) > [Spyware](#) 


[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Miscellaneous Offenses](#) > [Illegal Eavesdropping](#) > [General Overview](#) 


[Labor & Employment Law](#) > [Employee Privacy](#) > [Invasion of Privacy](#) 


**HN6** A valid distinction exists between a spyware program which simply breaks into a computer and retrieves information already stored on the hard drive, and a spyware program which copies the communication as it is transmitted and routes the copy to a storage file in the computer. [More Like This Headnote](#) | [Shepardize: Restrict By Headnote](#)

[Evidence](#) > [Illegal Eavesdropping](#) > [General Overview](#) 

**HN7** See [Fla. Stat. ch. 934.06](#) (2003).

[Computer & Internet Law](#) > [Criminal Offenses](#) > [Data Crimes & Fraud](#) 

[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Fraud](#) > [Computer Fraud](#) > [General Overview](#) 

[Evidence](#) > [Illegal Eavesdropping](#) > [General Overview](#) 

**HN8** Generally, the admission of evidence is a matter within the sound discretion of the trial court. [More Like This Headnote](#) | [Shepardize: Restrict By Headnote](#)

**COUNSEL:** Ryan Thomas Truskoski of Ryan Thomas Truskoski, P.A., Orlando, for Appellant.

David F. Allen, Winter Park, for Appellee.

**JUDGES:** SAWAYA, C.J. SHARP, W. and MONACO, JJ., concur.

**OPINION BY:** SAWAYA

OPINION

[\*1134] SAWAYA, C.J.

Emanating from a rather contentious divorce proceeding is an issue we must resolve regarding application of certain provisions of the Security of Communications Act (the Act) found in [Chapter 934, Florida Statutes](#) (2003). Specifically, we must determine whether the trial court properly concluded that pursuant to [section 934.03\(1\), Florida Statutes](#) (2003), certain communications were inadmissible because they were illegally intercepted by the Wife who, unbeknownst to the Husband, had installed a spyware program on a computer used by the Husband that copied and stored electronic communications between the Husband and another woman.

When marital discord erupted between the Husband and the Wife, the Wife secretly installed a spyware program called Spector on the Husband's computer. It is undisputed that **[\*\*2]** the Husband engaged in private on-line chats with another woman while playing Yahoo Dominoes on his computer. The Spector spyware secretly took snapshots of what appeared on the computer screen, and the frequency of these snapshots allowed Spector to capture and record all chat conversations, instant messages, e-mails sent and received, and the websites visited by the user of the computer. When the Husband discovered the Wife's clandestine attempt to monitor and record his conversations with his Dominoes partner, the Husband uninstalled the Spector software and filed a Motion for Temporary Injunction, which was subsequently granted, to prevent the Wife from disclosing the communications. Thereafter, the Husband requested and received a permanent injunction to prevent the Wife's disclosure of the communications and to prevent her from engaging in this activity in the future. The latter motion also requested that the trial court preclude introduction of the communications into evidence in the divorce proceeding. This request was also granted. The trial court, without considering the communications, entered a final judgment of dissolution of marriage. The Wife moved for rehearing, which **[\*\*3]** was subsequently denied.

The Wife appeals the order granting the permanent injunction, the final judgment, and the order denying the Wife's motion for rehearing on the narrow issue of whether the trial court erred in refusing to admit evidence of the Husband's computer activities obtained through the spyware the Wife secretly installed on the computer. The Wife argues that the electronic communications do not fall under the umbra of the Act because these communications were retrieved from storage and, therefore, are not "intercepted communications" as defined by the Act. In opposition, the Husband contends that the Spector spyware installed on the computer acquired his electronic communications real-time as they were in transmission and, therefore, are intercepts

illegally obtained under the Act.

The trial court found that the electronic communications were illegally obtained in violation of [section 934.03\(1\)\(a\)-\(e\)](#), and so we begin our analysis with the pertinent provisions of that statute, which subjects any person to criminal penalties who engages in the following activities:

<sup>HN1</sup> (a) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or **[\*\*4]** 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, **[\*\*1135]** or other device to intercept any oral communication when:

1. Such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

2. Such device transmits communications by radio or interferes with the transmission of such communication;

(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) Intentionally discloses, or endeavors to disclose, to any other person the contents of any **[\*\*5]** wire, oral, or electronic communication intercepted by means authorized by subparagraph (2)(a)2., paragraph (2)(b), paragraph (2)(c), s. 934.07, or s. 934.09 when that person knows or has reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, has obtained or received the information in connection with a criminal investigation, and intends to improperly obstruct, impede, or interfere with a duly authorized criminal investigation;

shall be punished as provided in subsection (4).

[§ 934.03\(1\)\(a\)-\(e\), Fla. Stat. \(2003\)](#). <sup>HN2</sup> Enactment of these prohibitions connotes "a policy decision by the Florida legislature to allow each party to a conversation to have an expectation of privacy from interception by another party to the conversation." [Shevin v. Sunbeam Television Corp.](#), 351 So. 2d 723, 726-27 (Fla. 1977). The purpose of the Act is to protect every person's right to privacy and to prevent the pernicious effect on all citizens who would otherwise feel insecure from intrusion into their private conversations and communications. *Id.*

<sup>HN3</sup> The clear intent of the Legislature in enacting **[\*\*6]** [section 934.03](#) was to make it illegal for a person to intercept wire, oral, or electronic communications. It is beyond doubt that what the trial court excluded from evidence are "electronic communications."<sup>1</sup> The core of the issue lies in whether the electronic communications were intercepted. <sup>HN4</sup> The term "intercept" is defined by the Act as "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." [§ 934.02\(3\), Fla. Stat. \(2003\)](#). We discern that there is a rather fine distinction between what is transmitted as an electronic communication subject to interception and the storage of what has been previously communicated. It is here that we tread upon new ground. Because we have found no precedent rendered by the Florida courts that considers this distinction, and in light of the fact that the Act was modeled after the Federal Wiretap Act,<sup>2</sup> we advert to decisions by the **[\*\*1136]** federal courts that have addressed this issue for guidance.<sup>3</sup>

#### FOOTNOTES

<sup>1</sup> <sup>HN5</sup> The term "electronic communications" is defined in [section 934.02\(12\), Florida Statutes \(2003\)](#), as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects intrastate, inter-state, or foreign commerce . . ." **[\*\*7]**

<sup>2</sup> What we label the Federal Wiretap Act is found in [18 U.S.C. § 2510, et seq.](#), as amended by Title I of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, Title I, 100 Stat. 1848 (1986).

<sup>3</sup> See [Jackson v. State](#), 636 So. 2d 1372, 1374 (Fla. 2d DCA 1994) (stating, in reference to the Act, that "we also examine its interpretation by the federal courts under Florida's established rule of statutory construction 'which recognizes that if a state law is patterned after a federal law on the same subject, the Florida law will be accorded the same construction as in the federal courts to the extent the construction is harmonious with the spirit of the Florida legislation.'" (quoting [O'Loughlin v. Pinchback](#), 579 So. 2d 788, 791 (Fla. 1st DCA 1991)), *approved*, 650 So. 2d 24 (Fla. 1995).

The federal courts have consistently held that electronic communications, in order to be intercepted, must be acquired contemporaneously with transmission and that electronic communications are not intercepted within the **[\*\*8]** meaning of the

Federal Wiretap Act if they are retrieved from storage. See *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3d Cir. 2003); *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir.), cert. denied, 543 U.S. 813, 160 L. Ed. 2d 17, 125 S. Ct. 48 (2004); *United States v. Steiger*, 318 F.3d 1039 (11th Cir.), cert. denied, 538 U.S. 1051, 155 L. Ed. 2d 1095, 123 S. Ct. 2120 (2003); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002), cert. denied, 537 U.S. 1193, 154 L. Ed. 2d 1028, 123 S. Ct. 1292 (2003). These courts arrived at this conclusion based on the federal law definitions of (1) the term "intercept," which is very similar to the definition in the Florida Act, (2) the term "wire communication," which provides for electronic storage, and (3) the term "electronic communication," which does not provide for electronic storage. The fact that the definition of "wire communication" provides for electronic storage while the definition of "electronic communication" does not, suggests to the federal courts that Congress intended "intercept" to include retrieval from storage of wire communications, but exclude **[\*\*9]** retrieval from storage of electronic communications. The definition of "wire communication" in the Florida Act, unlike the Federal Wiretap Act, does not include a provision for retrieval from storage and, therefore, it is not clear whether the same rationale would be applied by the federal courts to provisions identical to the Florida Act. However, we need not decide whether electronic communications may never be intercepted from storage under the Florida Act because the particular facts and circumstances of the instant case reveal that the electronic communications were intercepted contemporaneously with transmission.

The Spector spyware program that the Wife surreptitiously installed on the computer used by the Husband intercepted and copied the electronic communications as they were transmitted. We believe that particular method constitutes interception within the meaning of the Florida Act, and the decision in *Steiger* supports this conclusion. In *Steiger*, an individual was able to hack into the defendant's computer via a Trojan horse virus that allowed the hacker access to pornographic materials stored on the hard drive. The hacker was successful in transferring the pornographic **[\*\*10]** material from that computer to the hacker's computer. The court held that because the Trojan horse virus simply copied information that had previously been stored on the computer's hard drive, the capture of the electronic communication was not an interception within the meaning of the Federal Wiretap Act. The court did indicate, however, that interception could occur if the virus or software intercepted **[\*\*1137]** the communication as it was being transmitted and copied it. The court stated:

There is only a narrow window during which an E-mail interception may occur--the seconds or milli-seconds before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.

*Steiger*, 318 F.3d at 1050 (quoting Jarrod J. White, *E-Mail at Work.com: Employer Monitoring of Employee E-Mail*, 48 *Aia. L. Rev.* 1079, 1083 (1997)). Hence, <sup>HNS</sup> a valid distinction exists between a spyware **[\*\*11]** program similar to that in *Steiger*, which simply breaks into a computer and retrieves information already stored on the hard drive, and a spyware program similar to the one installed by the Wife in the instant case, which copies the communication as it is transmitted and routes the copy to a storage file in the computer.

The Wife argues that the communications were in fact stored before acquisition because once the text image became visible on the screen, the communication was no longer in transit and, therefore, not subject to intercept. We disagree. We do not believe that this evanescent time period is sufficient to transform acquisition of the communications from a contemporaneous interception to retrieval from electronic storage. We conclude that because the spyware installed by the Wife intercepted the electronic communication contemporaneously with transmission, copied it, and routed the copy to a file in the computer's hard drive, the electronic communications were intercepted in violation of the Florida Act.

We must next determine whether the improperly intercepted electronic communications may be excluded from evidence under the Act. The exclusionary provisions of **[\*\*12]** the Act are found in section 934.06, Florida Statutes (2003), which provides that <sup>HNS</sup> 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 . . . . Conspicuously absent from the provisions of this statute is any reference to electronic communications. The federal courts, which interpreted an identical statute contained in the Federal Wiretap Act, have held that because provision is not made for exclusion of intercepted electronic communications, Congress intended that such communications not be excluded under the Federal Wiretap Act. See *Steiger*. We agree with this reasoning and conclude that the intercepted electronic communications in the instant case are not excludable under the Act. But this does not end the inquiry.


Although not specifically excludable under the Act, it is illegal and punishable as a crime under the Act to intercept electronic communications. § 934.03, Fla. Stat. (2003). The trial court found that the electronic communications were illegally intercepted in violation of the Act and ordered that they not be admitted in evidence. <sup>HNS</sup> Generally, the **[\*\*13]** admission of evidence is a matter within the sound discretion of the trial court. See *Stewart & Stevenson Servs., Inc. v. Westchester Fire Ins. Co.*, 804 So. 2d 584, 587 (Fla. 5th DCA 2002); *Forester v. Norman Roger Jewell & Brooks Int'l, Inc.*, 610 So. 2d 1369, 1372 (Fla. 1st DCA 1992) ("The admission of evidence is within the sound judicial discretion of the trial judge, whose decision in such regard must be viewed in the context of the entire trial.") (citation omitted); see also *Globe v. State*, 877 So. 2d 663, 672 **[\*\*1138]** (Fla. 2004) ("A trial judge's ruling on the admissibility of evidence will not be disturbed absent an abuse of discretion.") (quoting *Blanco v. State*, 452 So. 2d 520 (Fla. 1984), cert. denied, 469 U.S. 1181, 83 L. Ed. 2d 953, 105 S. Ct. 940 (1985)); *Shearon v. Sullivan*, 821 So. 2d 1222, 1225 (Fla. 1st DCA 2002) ("The standard of review of a trial court's exclusion of evidence is abuse of discretion") (citation omitted). Because the evidence was illegally obtained, we conclude that the trial court did not abuse its discretion in refusing to admit it. See *Daniels v. State*, 381 So. 2d 707 (Fla. 1st DCA 1979), **[\*\*14]** *aff'd*, 389 So. 2d 631 (1980); *Horn v. State*, 298 So. 2d 194 (Fla. 1st DCA 1974), cert. denied, 308 So. 2d 117 (Fla. 1975).

We affirm the orders and the final judgment under review in the instant case.

AFFIRMED.

SHARP, W. and MONACO, JJ., concur.









Source: [Legal](#) > / ... / > **FL State Cases, Combined** 

Terms: **"o'brien v. o'brien"** ([Edit Search](#) | [Suggest Terms for My Search](#))

View: Full

Date/Time: Monday, November 16, 2009 - 9:37 AM EST

\* Signal Legend:

-  - Warning: Negative treatment is indicated
-  - Questioned: Validity questioned by citing refs
-  - Caution: Possible negative treatment
-  - Positive treatment is indicated
-  - Citing Refs. With Analysis Available
-  - Citation information available

\* Click on any *Shepard's* signal to *Shepardize*® that case.

[My Lexis™](#) | [Search](#) | [Research Tasks](#) | [Get a Document](#) | [Shepard's®](#) | [Alerts](#) | [Total Litigator](#) | [Transactional Advisor](#) | [Counsel Selector](#)  
[History](#) | [Delivery Manager](#) | [Switch Client](#) | [Preferences](#) | [Sign Out](#) | [Help](#)



LexisNexis®

[About LexisNexis](#) | [Terms & Conditions](#) | [Contact Us](#)

[Copyright ©](#) 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

18 Pa.C.S. § 5702

PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS(R)

\*THIS DOCUMENT IS CURRENT THROUGH ACTS 2009-36, AND 38 TO 40 OF THE 2009 REGULAR SESSION\*

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER A. GENERAL PROVISIONS

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5702 (2009)

§ 5702. Definitions

As used in this chapter, the following words and phrases shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"AGGRIEVED PERSON." A person who was a party to any intercepted wire, electronic or oral communication or a person against whom the interception was directed.

"AURAL TRANSFER." A transfer containing the human voice at any point between and including the point of origin and the point of reception.

"COMMUNICATION COMMON CARRIER." Any person engaged as a common carrier for hire, in intrastate, interstate or foreign communication by wire or radio or in intrastate, interstate or foreign radio transmission of energy; however, a person engaged in radio broadcasting shall not, while so engaged, be deemed a common carrier.

"CONTENTS." As used with respect to any wire, electronic or oral communication, is any information concerning the substance, purport, or meaning of that communication.

"COURT." The Superior Court. For the purposes of Subchapter C only, the term shall mean the court of common pleas.

"ELECTRONIC COMMUNICATION." 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 photo-optical system, except:

- (1) Deleted.
- (2) Any wire or oral communication.
- (3) Any communication made through a tone-only paging device.
- (4) Any communication from a tracking device (as defined in this

section).

"ELECTRONIC COMMUNICATION SERVICE." Any service which provides to users the ability to send or receive wire or electronic communications.

"ELECTRONIC COMMUNICATION SYSTEM." Any wire, radio, electromagnetic, photo-optical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

"ELECTRONIC, MECHANICAL OR OTHER DEVICE." Any device or apparatus, including, but not limited to, an induction coil or a telecommunication identification interception device, that can be used to intercept a wire, electronic or oral communication other than:

(1) Any telephone or telegraph instrument, equipment or facility, or any component thereof, furnished to the subscriber or user by a provider of wire or electronic communication service 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 being used by a communication common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties.

(2) A hearing aid or similar device being used to correct subnormal hearing to not better than normal.

(3) Equipment or devices used to conduct interceptions under section 5704(15) (relating to exceptions to prohibition of interception and disclosure of communications).

"ELECTRONIC STORAGE."

(1) Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof.

(2) Any storage of such a communication by an electronic communication service for purpose of backup protection of the communication.

"HOME." The residence of a nonconsenting party to an interception, provided that access to the residence is not generally permitted to members of the public and the party has a reasonable expectation of privacy in the residence under the circumstances.

"IN-PROGRESS TRACE." The determination of the origin of a telephonic communication to a known telephone during an interception.

"INTERCEPT." Aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device. The term shall include the point at which the contents of the communication are monitored by investigative or law enforcement officers.

"INVESTIGATIVE OR LAW ENFORCEMENT OFFICER." Any officer of the United States, of another state or political subdivision thereof, or of the Commonwealth or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter or an equivalent crime in another jurisdiction, and any attorney authorized by law to prosecute or participate in the prosecution of such offense.

"JUDGE." When referring to a judge authorized to receive applications for, and to enter, orders authorizing interceptions of wire, electronic or oral communications pursuant to Subchapter B (relating to wire, electronic or oral communication), any judge of the Superior Court.

"ONE CALL SYSTEM." A communication system established by users to provide a single telephone number for contractors or designers or any other person to call notifying users of the caller's intent to engage in demolition or excavation work.

"ORAL COMMUNICATION." Any oral communication uttered by a person possessing an expectation that such communication is not subject to interception under circumstances justifying such expectation. The term does not include any electronic communication.

"ORGANIZED CRIME."

(1) The unlawful activity of an association trafficking in illegal goods or services, including but not limited to, gambling, prostitution, loan sharking, controlled substances, labor racketeering, or other unlawful activities; or

(2) any continuing criminal conspiracy or other unlawful practice which has as its objective:

(i) large economic gain through fraudulent or coercive practices; or

(ii) improper governmental influence.

"PEN REGISTER." A device which is used to capture, record or decode electronic or other impulses which identify the numbers dialed or otherwise transmitted, with respect to wire or electronic communications, on the targeted telephone. The term includes a device which is used to record or decode electronic or other impulses which identify the existence of incoming and outgoing wire or electronic communications on the targeted telephone. The term does not include a device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communication service provided by the provider, or any device used by a provider, or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of business.

"PERSON." 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.

"READILY ACCESSIBLE TO THE GENERAL PUBLIC." As used with respect to a radio communication, that such communication is not:

(1) scrambled or encrypted;

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

(3) carried on a subscriber or other signal subsidiary to a radio transmission;

(4) transmitted over a communication system provided by a common carrier, unless the communication is a tone-only paging system

communication; or

(5) transmitted on frequencies allocated under 47 CFR Parts 25, 74D, E, F or 94, unless, in the case of a communication transmitted on a frequency allocated under Part 74 which is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio.

"REMOTE COMPUTING SERVICE." The provision to the public of computer storage or processing services by means of an electronic communications system.

"STATE." Any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico and any territory or possession of the United States.

"SUSPECTED CRIMINAL ACTIVITY." A particular offense that has been, is or is about to occur as set forth under section 5709(3)(ii) (relating to application for order), any communications to be intercepted as set forth under section 5709(3)(iii) or any of the criminal activity set forth under section 5709(3)(iv) establishing probable cause for the issuance of an order.

"TELECOMMUNICATION IDENTIFICATION INTERCEPTION DEVICE." Any equipment or device capable of intercepting any electronic communication which contains any electronic serial number, mobile identification number, personal identification number or other identification number assigned by a telecommunication service provider for activation or operation of a telecommunication device.

"TRACKING DEVICE." An electronic or mechanical device which permits only the tracking of the movement of a person or object.

"TRAP AND TRACE DEVICE." A device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.

"USER." Any person or entity who:

(1) uses an electronic communication service; and

(2) is duly authorized by the provider of the service to engage in the use.

"WIRE COMMUNICATION." Any aural transfer made in whole or in part through the use of facilities for the transmission of communication by wire, cable or other like connection between the point of origin and the point of reception, including the use of such a connection in a switching station, furnished or operated by a telephone, telegraph or radio company for hire as a communication common carrier. The term includes any electronic storage of such communication.

**HISTORY:** Act 1988-115 (S.B. 797), § 3, approved Oct. 21, 1988, eff. immediately; Act 1998-19 (S.B. 635), § 5, approved Feb. 18, 1998, eff. immediately; Act 2002-162 (H.B. 976), § 3, approved Dec. 9, 2002, eff. in 60 days..

LexisNexis (R) Notes:

18 Pa.C.S. § 5703

PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS(R)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*  
\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*  
\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5703 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5703. Interception, disclosure or use of wire, electronic or oral communications

Except as otherwise provided in this chapter, a person is guilty of a felony of the third degree if he:

- (1) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or oral communication;
- (2) intentionally discloses or endeavors to disclose to any other person the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication; or
- (3) intentionally uses or endeavors to use the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know, that the information was obtained through the interception of a wire, electronic or oral communication.

**HISTORY:** Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately.

LexisNexis (R) Notes:

☞ CASE NOTES



18 Pa.C.S. § 5704

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

[Case Notes](#)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF  
THE 2009 REGULAR SESSION\*

Resources & Practice Tools

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT  
THROUGH ACT 36\*

Law Reviews

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

> 67 Temp. L. Rev. 1051,  
INDIVIDUAL RIGHTS AND THE  
PENNSYLVANIA CONSTITUTION: IS  
THERE THERE A STATE STATE  
ACTION REQUIREMENT?

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND  
DECENCY

> 64 U. Pitt. L. Rev. 855, HOLD THE  
PHONE: PA HIGH COURT SAYS NO  
REASONABLE EXPECTATION OF  
PRIVACY DURING PHONE CALL.

CHAPTER 57. WIRETAPPING AND ELECTRONIC  
SURVEILLANCE

> 6 Widener J. Pub. L. 885, ANNUAL  
SURVEY OF PENNSYLVANIA  
ADMINISTRATIVE LAW: SURVEY OF  
SELECTED COURT DECISIONS:  
PUBLIC UTILITIES: *United  
Telephone Co. v. Pennsylvania  
Public Utility Commission: The  
Commonwealth Court Strictly  
Construes the Provisions of the  
Pennsylvania Wiretapping and  
Electronic Surveillance Control Act.*

SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL  
COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5704 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5704. Exceptions to prohibition of interception and disclosure of communications

It shall not be unlawful and no prior court approval shall be required under this chapter for:

(1) An operator of a switchboard, or an officer, agent or employee of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of wire or electronic communication service. However, no provider of wire or electronic communication service shall utilize service observing or random monitoring except for mechanical or service quality control checks.

(2) Any investigative or law enforcement officer or any person acting at the direction or request of an investigative or law enforcement officer to intercept a wire, electronic or oral communication involving suspected criminal activities, including, but not limited to, the crimes enumerated in section 5708 (relating to order authorizing interception of wire, electronic or oral communications), where:

(i) Deleted.

(ii) one of the parties to the communication has given prior consent to such interception. However, no interception under this paragraph shall be made unless the Attorney General or a deputy attorney general designated in writing by the Attorney General, or the district attorney, or an assistant district attorney designated in writing by the district attorney, of the county wherein the interception is to be made, has reviewed the facts and is satisfied that the consent is voluntary and has given prior approval for the interception; however such interception shall be subject to the recording and record keeping requirements of section 5714(a) (relating to recording of intercepted communications) and that the Attorney General, deputy attorney general, district attorney or assistant district attorney authorizing the interception shall be the custodian of recorded evidence obtained therefrom;

(iii) the investigative or law enforcement officer meets in person with a suspected felon and wears a concealed electronic or mechanical device capable of intercepting or recording oral communications. However, no interception under this subparagraph may be used in any criminal prosecution except for a prosecution involving harm done to the investigative or law enforcement officer. This subparagraph shall not be construed to limit the interception and disclosure authority provided for in this subchapter; or

(iv) the requirements of this subparagraph are met. If an oral interception otherwise authorized under this paragraph will take place in the home of a nonconsenting party, then, in addition to the requirements of subparagraph (ii), the interception shall not be conducted until an order is first obtained from the president judge, or his designee who shall also be a judge, of a court of common pleas, authorizing such in-home interception, based upon an affidavit by an investigative or law enforcement officer that establishes probable cause for the issuance of such an order. No such order or affidavit shall be required where probable cause and exigent circumstances exist. For the purposes of this paragraph, an oral interception shall be deemed to take place in the home of a nonconsenting party only if both the consenting and nonconsenting parties are physically present in the home at the time of the interception.

(3) Police and emergency communications systems to record telephone communications coming into and going out of the communications system of the Pennsylvania Emergency Management Agency or a police department, fire department or county emergency center, if:

(i) the telephones thereof are limited to the exclusive use of the communication system for administrative purposes and provided the communication system employs a periodic warning which indicates to the parties to the conversation that the call is being recorded;

(ii) all recordings made pursuant to this clause, all notes made therefrom, and all transcriptions thereof may be destroyed at any time, unless required with regard to a pending matter; and



(iii) at least one nonrecorded telephone line is made available for public use at the Pennsylvania Emergency Management Agency and at each police department, fire department or county emergency center.

(4) A person, to intercept a wire, electronic or oral communication, where all parties to the communication have given prior consent to such interception.

(5) Any investigative or law enforcement officer, or communication common carrier acting at the direction of an investigative or law enforcement officer or in the normal course of its business, to use a pen register, trap and trace device, or telecommunication identification interception device as provided in Subchapter E (relating to pen registers, trap and trace devices and telecommunication identification interception devices).

(6) Personnel of any public utility to record telephone conversations with utility customers or the general public relating to receiving and dispatching of emergency and service calls provided there is, during such recording, a periodic warning which indicates to the parties to the conversation that the call is being recorded.

(7) A user, or any officer, employee or agent of such user, to record telephone communications between himself and a contractor or designer, or any officer, employee or agent of such contractor or designer, pertaining to excavation or demolition work or other related matters, if the user or its agent indicates to the parties to the conversation that the call will be or is being recorded. As used in this paragraph, the terms "user," "contractor," "demolition work," "designer" and "excavation work" shall have the meanings given to them in the act of December 10, 1974 (P.L. 852, No. 287), referred to as the Underground Utility Line Protection Law; and a one call system shall be considered for this purpose to be an agent of any user which is a member thereof.

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

(9) A person or entity providing electronic communication service to the public to divulge the contents of any such communication:

(i) as otherwise authorized in this section or section 5717 (relating to investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence);

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

(iii) to a person employed or authorized, or whose facilities are used, to forward the 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.

A person or entity providing electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one directed to the person or entity, or an agent thereof) while in transmission of that service to any person or entity other than an addressee or intended recipient of the communication or an agent of the addressee or intended recipient.

(10) Any person:

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

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

(A) by a station for the use of the general public, or which relates to ships, aircraft, vehicles or persons in distress;

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

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

(D) by any marine or aeronautical communication system;

(iii) to engage in any conduct which:

(a) is prohibited by section 633 of the Communications Act of 1934 (48 Stat. 1105, 47 U.S.C. § 553); or

(b) is excepted from the application of section 705(a) of the Communications Act of 1934 (47 U.S.C. § 605(a)) by section 705(b) of that act (47 U.S.C. § 605(b)); or

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

(11) Other users of the same frequency to intercept any radio communication made through a system which utilizes frequencies monitored by individuals engaged in the provisions or use of the system, if the communication is not scrambled or encrypted.

(12) Any investigative or law enforcement officer or any person acting at the direction or request of an investigative or law enforcement officer to intercept a wire or oral communication involving suspected criminal activities where the officer or the person is a party to the communication and there is reasonable cause to believe that:

(i) the other party to the communication is either:

(A) holding a hostage; or

(B) has barricaded himself and taken a position of confinement to avoid apprehension; and

(ii) that party:

(A) will resist with the use of weapons; or

(B) is threatening suicide or harm to others.

(13) An investigative officer, a law enforcement officer or employees of the Department of Corrections for State correctional facilities to intercept, record, monitor or divulge any telephone calls from or to an inmate in a facility under the following conditions:

(i) The Department of Corrections shall adhere to the following procedures and restrictions when intercepting, recording, monitoring or divulging any telephone calls from or to an inmate in a State correctional facility as provided for by this paragraph:

(A) Before the implementation of this paragraph, all inmates of the facility shall be notified in writing that, as of the effective date of this paragraph, their telephone conversations may be intercepted, recorded, monitored or divulged.

(B) Unless otherwise provided for in this paragraph, after intercepting or recording a telephone conversation, only the superintendent, warden or a designee of the superintendent or warden or other chief administrative official or his or her designee shall have access to that recording.

(C) The contents of an intercepted and recorded telephone conversation shall be divulged only as is necessary to safeguard the orderly operation of the facility, in response to a court order or in the prosecution or investigation of any crime.

(ii) So as to safeguard the attorney-client privilege, the Department of Corrections shall not intercept, record, monitor or divulge any conversation between an inmate and an attorney.

(iii) Persons who are calling in to a facility to speak to an inmate shall be notified that the call may be recorded or monitored.

(iv) The Department of Corrections shall promulgate guidelines to implement the provisions of this paragraph for State correctional facilities.

(14) An investigative officer, a law enforcement officer or employees of a county correctional facility to intercept, record, monitor or divulge any telephone calls from or to an inmate in a facility under the following conditions:

(i) The county correctional facility shall adhere to the following

procedures and restrictions when intercepting, recording, monitoring or divulging any telephone calls from or to an inmate in a county correctional facility as provided for by this paragraph:

(A) Before the implementation of this paragraph, all inmates of the facility shall be notified in writing that, as of the effective date of this paragraph, their telephone conversations may be intercepted, recorded, monitored or divulged.

(B) Unless otherwise provided for in this paragraph, after intercepting or recording a telephone conversation, only the superintendent, warden or a designee of the superintendent or warden or other chief administrative official or his or her designee shall have access to that recording.

(C) The contents of an intercepted and recorded telephone conversation shall be divulged only as is necessary to safeguard the orderly operation of the facility, in response to a court order or in the prosecution or investigation of any crime.

(ii) So as to safeguard the attorney-client privilege, the county correctional facility shall not intercept, record, monitor or divulge any conversation between an inmate and an attorney.

(iii) Persons who are calling into a facility to speak to an inmate shall be notified that the call may be recorded or monitored.

(iv) The superintendent, warden or a designee of the superintendent or warden or other chief administrative official of the county correctional system shall promulgate guidelines to implement the provisions of this paragraph for county correctional facilities.

(15) The personnel of a business engaged in telephone marketing or telephone customer service by means of wire, oral or electronic communication to intercept such marketing or customer service communications where such interception is made for the sole purpose of training, quality control or monitoring by the business, provided that one party involved in the communications has consented to such intercept. Any communications recorded pursuant to this paragraph may only be used by the business for the purpose of training or quality control. Unless otherwise required by Federal or State law, communications recorded pursuant to this paragraph shall be destroyed within one year from the date of recording.

(16) A law enforcement officer, whether or not certified under section 5724 (relating to training), acting in the performance of his official duties to intercept and record an oral communication between individuals in accordance with the following:

(i) At the time of the interception, the oral communication does not occur inside the residence of any of the individuals.

(ii) At the time of the interception, the law enforcement officer:

(A) is operating the visual or audible warning system of the law enforcement officer's vehicle authorized by 75 Pa.C.S. § 4571

(relating to visual and audible signals on emergency vehicles) or is clearly identifiable as a law enforcement officer;

(B) is in close proximity to the individuals' oral communication;

(C) is using an electronic, mechanical or other device which has been approved under section 5706(b) (4)(relating to exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices) to intercept the oral communication, the recorder of which is mounted in the law enforcement officer's vehicle; and

(D) informs, as soon as reasonably practicable, the individuals identifiably present that he has intercepted and recorded the oral communication.

(iii) As used in this paragraph, the following words and phrases shall have the meanings given to them in this subparagraph:

"Law enforcement officer." A member of the Pennsylvania State Police or an individual employed as a police officer who holds a current certificate under 53 Pa.C.S. Ch. 21 Subch. D (relating to municipal police education and training).

"Recorder." An electronic, mechanical or other device used to store an oral communication on tape or on some other comparable medium.

#### **History:**

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately; Act 1995 Special Session-20 (H.B. 127), § 2, approved Sept. 26, 1995, eff. in 60 days; Act 1996-186 (H.B. 2592), § 1, approved Dec. 19, 1996, eff. in 60 days; Act 1998-19 (S.B. 635), § 6, approved Feb. 18, 1998, eff. immediately; Act 2002-52 (S.B. 369), § 1, approved June 6, 2002, eff. immediately..

#### **NOTES:**

PENNSYLVANIA ADMINISTRATIVE CODE REFERENCES.

1. 37 Pa. Code § 93.7 (2009), PART AGENCIES AND OFFICES.
2. 37 Pa. Code § 95.233a (2009), PART AGENCIES AND OFFICES.

LexisNexis (R) Notes:

#### **Case Notes:**

18 Pa.C.S. § 5705

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

[Case Notes](#)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF  
THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5705 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5705. Possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices

Except as otherwise specifically provided in section 5706 (relating to exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices), a person is guilty of a felony of the third degree if he does any of the following:

- (1) Intentionally possesses an 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 a wire, electronic or oral communication.
- (2) Intentionally sells, transfers or distributes an 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 a wire, electronic or oral communication.
- (3) Intentionally manufactures or assembles an 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 a wire, electronic or oral communication.
- (4) Intentionally places in any newspaper, magazine, handbill, or other publication any advertisement of an 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 a wire, electronic or oral communication or of an electronic, mechanical or other device where such advertisement promotes the use of such device for the purpose of the surreptitious interception of a wire, electronic or oral communication.

**History:**

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately.

LexisNexis (R) Notes:

**Case Notes:**



1. Because defendant tape recorded the victim's conversations at work, because the victim possessed a reasonable expectation of privacy with regard to the victim's conversations, and because defendant's method of recording did not discriminate between business conversations and personal conversations, there was sufficient evidence to find that defendant violated 18 Pa.C.S. §§ 5703(1), 5705(1), 907(A); accordingly, defendant was not entitled to pretrial habeas corpus relief. Commonwealth v. Ward, 2006 Pa. Dist. & Cnty. Dec. LEXIS 559 (Dec. 12, 2006).



2. Where appellant was charged under 18 Pa. C.S. § 5705(1) for possession of illegal wiretapping devices, the evidence was suppressed, because the warrant failed to provide a sufficient basis for an independent determination by a neutral judicial officer that probable cause existed. Commonwealth v. Kalinowski, 303 Pa. Super. 354, 449 A.2d 725, 1982 Pa. Super. LEXIS 5045 (1982).



3. Where appellant was charged under 18 Pa. C.S. § 5705(1) for possession of illegal wiretapping devices, the evidence was suppressed, because the warrant failed to provide a sufficient basis for an independent determination by a neutral judicial officer that probable

18 Pa.C.S. § 5706

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*  
\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*  
\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5706 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5706. Exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices

(a) UNLAWFUL ACTIVITIES.-- It shall not be unlawful under this chapter for:

(1) 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 the wire or electronic communication service; or

(2) a person under contract with the United States, the Commonwealth or a political subdivision thereof, a state or a political subdivision thereof, or an officer, agent or employee of the United States, the Commonwealth or a political subdivision thereof, or a state or a political subdivision thereof, to possess, sell, distribute, manufacture, assemble or advertise an electronic, mechanical or other device, while acting in furtherance of the appropriate activities of the United States, the Commonwealth or a political subdivision thereof, a state or a political subdivision thereof or a provider of wire or electronic communication service.

(b) RESPONSIBILITY.--

(1) Except as provided under paragraph (2), the Attorney General and the district attorney or their designees so designated in writing shall have the sole responsibility to buy, possess and loan any electronic, mechanical or other device which is to be used by investigative or law



enforcement officers for purposes of interception as authorized under section 5704(2), (5) and (12) (relating to exceptions to prohibition of interception and disclosure of communications), 5712 (relating to issuance of order and effect), 5713 (relating to emergency situations) or 5713.1 (relating to emergency hostage and barricade situations).


(2) The division or bureau or section of the Pennsylvania State Police responsible for conducting the training in the technical aspects of wiretapping and electronic surveillance as required by section 5724 (relating to training) may buy and possess any electronic, mechanical or other device which is to be used by investigative or law enforcement officers for purposes of interception as authorized under section 5704(2), (5) and (12), 5712, 5713 or 5713.1 for the purpose of training. However, any electronic, mechanical or other device bought or possessed under this provision may be loaned to or used by investigative or law enforcement officers for purposes of interception as authorized under section 5704(2), (5) and (12), 5712, 5713 or 5713.1 only upon written approval by the Attorney General or a deputy attorney general designated in writing by the Attorney General or the district attorney or an assistant district attorney designated in writing by the district attorney of the county wherein the suspected criminal activity has been, is or is about to occur.

(3) With the permission of the Attorney General or a district attorney who has designated any supervising law enforcement officer for purposes of interceptions as authorized under section 5713.1, the law enforcement agency which employs the supervising law enforcement officer may buy, possess, loan or borrow any electronic, mechanical or other device which is to be used by investigative or law enforcement officers at the direction of the supervising law enforcement officer solely for the purpose of interception as authorized under sections 5704(12) and 5713.1.

(4) The Pennsylvania State Police shall annually establish equipment standards for any electronic, mechanical or other device which is to be used by law enforcement officers for purposes of interception as authorized under section 5704(16). The equipment standards shall be published annually in the Pennsylvania Bulletin.

#### History:

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately; Act 1998-19 (S.B. 635), § 7, approved Feb. 18, 1998, eff. immediately; Act 2002-52 (S.B. 369), § 1, approved June 6, 2002, eff. immediately.; Act 2002-162 (H.B. 976), § 4, approved Dec. 9, 2002, eff. in 60 days..

Source: [Legal](#) > / . . . / > PA - Pennsylvania Statutes, Annotated by LexisNexis 

View: Full

Date/Time: Tuesday, October 27, 2009 - 4:16 PM EDT

18 Pa.C.S. § 5707

[Retrieve State Legislative Impact® \(\\$\)](#)

[Practitioner's Toolbox](#)



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*  
\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*  
\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5707 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5707. Seizure and forfeiture of electronic, mechanical or other devices

Any electronic, mechanical or other device possessed, used, sent, distributed, manufactured, or assembled in violation of this chapter is hereby declared to be contraband and may be seized and forfeited to the Commonwealth.

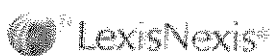
**History:**

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately.

Source: [Legal](#) > / . . . / > PA - Pennsylvania Statutes, Annotated by LexisNexis

View: Full

Date/Time: Tuesday, October 27, 2009 - 4:16 PM EDT



[About LexisNexis](#) | [Terms & Conditions](#) | [Contact Us](#)

Copyright © 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

18 Pa.C.S. § 5708

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox 

PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

 [Case Notes](#)

 [Opinions of Attorney General](#)

 [History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF  
THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT  
THROUGH ACT 36\*

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

Resources & Practice Tools

Law Reviews

> 33 Duq. L. Rev. 523, RECENT  
DEVELOPMENT: Recent  
Developments in Pennsylvania Law.

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES

PART II. DEFINITION OF SPECIFIC OFFENSES

ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY

CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE

SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5708 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5708. Order authorizing interception of wire, electronic or oral communications

The Attorney General, or, during the absence or incapacity of the Attorney General, a deputy attorney general designated in writing by the Attorney General, or the district attorney or, during the absence or incapacity of the district attorney, an assistant district attorney designated in writing by the district attorney of the county wherein the suspected criminal activity has been, is or is about to occur, may make written application to any Superior Court judge for an order authorizing the interception of a wire, electronic or oral communication by the investigative or law enforcement officers or agency having responsibility for an investigation involving suspected criminal activities when such interception may provide evidence of the commission of any of the following offenses, or may provide evidence aiding in the apprehension of the perpetrator or perpetrators of any of the following offenses:

(1) Under this title:

Section 911 (relating to corrupt organizations)

Section 2501 (relating to criminal homicide)

Section 2502 (relating to murder)

Section 2503 (relating to voluntary manslaughter)

Section 2702 (relating to aggravated assault)

Section 2706 (relating to terroristic threats)

Section 2709.1 (relating to stalking)

Section 2716 (relating to weapons of mass destruction)

Section 2901 (relating to kidnapping)

Section 3002 (relating to trafficking of persons)

Section 3121 (relating to rape)

Section 3123 (relating to involuntary deviate sexual intercourse)

Section 3124.1 (relating to sexual assault)

Section 3125 (relating to aggravated indecent assault)

Section 3301 (relating to arson and related offenses)

Section 3302 (relating to causing or risking catastrophe)

Section 3502 (relating to burglary)

Section 3701 (relating to robbery)

Section 3921 (relating to theft by unlawful taking or disposition)

Section 3922 (relating to theft by deception)

Section 3923 (relating to theft by extortion)

Section 4701 (relating to bribery in official and political matters)

Section 4702 (relating to threats and other improper influence in official and political matters)

Section 5512 (relating to lotteries, etc.)

Section 5513 (relating to gambling devices, gambling, etc.)

Section 5514 (relating to pool selling and bookmaking)

Section 5516 (relating to facsimile weapons of mass destruction)

Section 6318 (relating to unlawful contact with minor)

(2) Under this title, where such offense is dangerous to life, limb or property and punishable by imprisonment for more than one year:

Section 910 (relating to manufacture, distribution or possession of devices for theft of telecommunication services)

Section 2709(a)(4), (5), (6) or (7) (relating to harassment)

Section 3925 (relating to receiving stolen property) Section 3926 (relating to theft of services)

Section 3927 (relating to theft by failure to make required disposition of funds received)

Section 3933 (relating to unlawful use of computer) Section 4108 (relating to commercial bribery and breach of duty to act disinterestedly)

Section 4109 (relating to rigging publicly exhibited contest)

Section 4117 (relating to insurance fraud) Section 4305 (relating to dealing in infant children) Section 4902 (relating to perjury)

Section 4909 (relating to witness or informant taking bribe)

Section 4911 (relating to tampering with public records or information)

Section 4952 (relating to intimidation of witnesses or victims)

Section 4953 (relating to retaliation against witness or victim)

Section 5101 (relating to obstructing administration of law or other governmental function)

Section 5111 (relating to dealing in proceeds of unlawful activities)

Section 5121 (relating to escape)

Section 5902 (relating to prostitution and related offenses)

Section 5903 (relating to obscene and other sexual materials and performances)

Section 7313 (relating to buying or exchanging Federal food order coupons, stamps, authorization cards or access devices)

(3) Under the act of March 4, 1971 (P.L. 6, No. 2), known as the Tax Reform Code of 1971, where such offense is dangerous to life, limb or property and punishable by imprisonment for more than one year:

Section 1272 (relating to sales of unstamped cigarettes)

Section 1273 (relating to possession of unstamped cigarettes)

Section 1274 (relating to counterfeiting)

(4) Any offense set forth under section 13(a) of the act of April 14, 1972 (P.L. 233, No. 64), known as The Controlled Substance, Drug, Device and Cosmetic Act, not including the offense described in clause (31) of section 13(a).

(5) Any offense set forth under the act of November 15, 1972 (P.L. 1227, No. 272).

(6) Any conspiracy to commit any of the offenses set forth in this section.

(7) Under the act of, 1998 (P.L. 874, No. 110), known as the Motor Vehicle Chop Shop and Illegally Obtained and Altered Property Act.

**History:**

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately; Act 1990-3 (H.B. 682), § 1, approved Feb. 2, 1990, eff. immediately; Act 1998-145 (S.B. 1373), § 1, approved Dec. 21, 1998, eff. in 60 days; Act 1998-19 (S.B. 635), § 7, approved Feb. 18, 1998, eff. immediately; Act 2002-82 (S.B. 1109), § 5, approved June 28, 2002, eff. in 60 days.; Act 2002-134 (S.B. 834), § 1, approved Nov. 20, 2002, eff. in 60 days.; Act 2002-162 (H.B. 976), § 4, approved Dec. 9, 2002, eff. in 60 days.; Act 2002-218 (S.B. 1515), § 5, approved Dec. 9, 2002, eff. in 60 days.; Act 2006-139 (H.B. 1112), § 3, approved Nov. 9, 2006, eff. in 60 days..

LexisNexis (R) Notes:

**Case Notes:**



1. Sheriffs were not "investigative or law enforcement officers" under 18 Pa.C.S. § 5708 and therefore were not eligible to receive training and certification from the state police to conduct wiretap investigations; the common law power to arrest for breaches of the peace committed in one's presence did not provide support for the sheriffs' premise that they were empowered to conduct wiretapping; neither the Wiretapping and Electronic Surveillance Control Act nor statutory provisions regarding sheriffs, 42 Pa.C.S. § 2921 and 13 P.S. § 40, supported the sheriffs' claim. *Kopko v. Miller*, 586 Pa. 170, 892 A.2d 766, 2006 Pa. LEXIS 41 (2006).

2. Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. § 5701 et seq., that allowed wiretaps to investigate activities proscribed by the Corrupt Organizations statute, 18 Pa. Cons. Stat. § 911, in an action in which wiretap-obtained evidence was admitted into evidence, did not exceed the statutory authority granted to the states by 18 U.S.C.S. § 2516(2). *Commonwealth v. Birdseye*, 543 Pa. 251, 670 A.2d 1124, 1996 Pa. LEXIS 12 (1996), writ of certiorari denied by 518 U.S. 1019, 135 L. Ed. 2d 1071, 116 S. Ct. 2552, 1996 U.S. LEXIS 4095, 64 U.S.L.W. 3854 (1996).

18 Pa.C.S. § 5709

[Retrieve State Legislative Impact® \(\\$\)](#)

PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF  
THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT  
THROUGH ACT 36\*

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND  
DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC  
SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL  
COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5709 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will  
expire on December 31, 2013, unless extended by Statute.

§ 5709. Application for order

Each application for an order of authorization to intercept a wire, electronic or oral communication shall be made in writing upon the personal oath or affirmation of the Attorney General or a district attorney of the county wherein the suspected criminal activity has been, is or is about to occur and shall contain all of the following:

- (1) A statement of the authority of the applicant to make such application.
- (2) A statement of the identity and qualifications of the investigative or law enforcement officers or agency for whom the authority to intercept a wire, electronic or oral communication is sought.
- (3) A sworn statement by the investigative or law enforcement officer who has knowledge of relevant information justifying the application, which shall include:
  - (i) The identity of the particular person, if known, committing the offense and whose communications are to be intercepted.
  - (ii) The details as to the particular offense that has been, is

Practitioner's Toolbox 

 [Case Notes](#)

 [History](#)

Resources & Practice Tools

Treatises and Analytical  
Materials

- > 43 P.L.E., SEARCHES AND SEIZURES § 71, Pennsylvania Law Encyclopedia, SEARCHES AND SEIZURES, § 71. Generally; Definitions, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.
- > 43 P.L.E., SEARCHES AND SEIZURES § 72, Pennsylvania Law Encyclopedia, SEARCHES AND SEIZURES, § 72. Interception of Wire, Electronic, or Oral Communication, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.
- > 48 P.L.E., TELECOMMUNICATIONS § 2, Pennsylvania Law Encyclopedia, TELECOMMUNICATIONS, § 2. -- Intercepting Communications, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

being, or is about to be committed.

(iii) The particular type of communication to be intercepted.

(iv) A showing that there is probable cause to believe that such communication will be communicated on the wire communication facility involved or at the particular place where the oral communication is to be intercepted.

(v) The character and location of the particular wire communication facility involved or the particular place where the oral communication is to be intercepted.

(vi) A statement of the period of time for which the interception is required to be maintained, and, if the character 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 statement of facts establishing probable cause to believe that additional communications of the same type will occur thereafter.

(vii) A particular statement of facts showing that other normal investigative procedures with respect to the offense have been tried and have failed, or reasonably appear to be unlikely to succeed if tried or are too dangerous to employ.

(4) Where the application is for the renewal or extension of an order, a particular statement of facts showing the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(5) A complete statement of the facts concerning all previous applications, known to the applicant made to any court for authorization to intercept a wire, electronic or oral communication involving any of the same facilities or places specified in the application or involving any person whose communication is to be intercepted, and the action taken by the court on each such application.

(6) A proposed order of authorization for consideration by the judge.

(7) Such additional testimony or documentary evidence in support of the application as the judge may require.

 **History:**

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately; Act 2002-162 (H.B. 976), § 4, approved Dec. 9, 2002, eff. in 60 days..

LexisNexis (R) Notes:



18 Pa.C.S. § 5710

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS (R)

[Case Notes](#)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

Resources & Practice Tools

Treatises and Analytical Materials

> 43 P.L.E., SEARCHES AND SEIZURES § 72, Pennsylvania Law Encyclopedia, SEARCHES AND SEIZURES, § 72. Interception of Wire, Electronic, or Oral Communication, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5710 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5710. Grounds for entry of order

(a) APPLICATION.-- Upon consideration of an application, the judge may enter an ex parte order, as requested or as modified, authorizing the interception of wire, electronic or oral communications anywhere within the Commonwealth, if the judge determines on the basis of the facts submitted by the applicant that there is probable cause for belief that all the following conditions exist:

(1) the person whose communications are to be intercepted is committing, has or had committed or is about to commit an offense as provided in section 5708 (relating to order authorizing interception of wire, electronic or oral communications);

(2) particular communications concerning such offense may be obtained through such interception;

(3) normal investigative procedures with respect to such offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ;

(4) the facility from which, or the place where, the wire, electronic or oral communications are to be intercepted, is, has been, or is about to be used, in connection with the commission of such offense, or is leased to, listed in the name of, or commonly used by, such person;

(5) the investigative or law enforcement officers or agency to be authorized to intercept the wire, electronic or oral communications are qualified by training and experience to execute the interception sought, and are certified under section 5724 (relating to training); and

(6) in the case of an application, other than a renewal or extension, for an order to intercept a communication of a person or on a facility which was the subject of a previous order authorizing interception, the application is based upon new evidence or information different from and in addition to the evidence or information offered to support the prior order, regardless of whether such evidence was derived from prior interceptions or from other sources.

(b) CORROBORATIVE EVIDENCE.-- As part of the consideration of an application in which there is no corroborative evidence offered, the judge may inquire in camera as to the identity of any informants or any other additional information concerning the basis upon which the investigative or law enforcement officer or agency has applied for the order of authorization which the judge finds relevant in order to determine if there is probable cause pursuant to this section.

 **History:**

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately.

**NOTES:**

PENNSYLVANIA ADMINISTRATIVE CODE REFERENCES.

1. 210 Pa. Code § 65.59 (2009), PART INTERNAL OPERATING PROCEDURES.

LexisNexis (R) Notes:

 **Case Notes:**



18 Pa.C.S. § 5711

Retrieve State Legislative Impact® (\$)

PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS(R)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*  
\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*  
\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION


**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5711 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5711. Privileged communications

No otherwise privileged communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

Source: [Legal](#) > / . . . / > **PA - Pennsylvania Statutes, Annotated by LexisNexis**   
View: Full  
Date/Time: Tuesday, October 27, 2009 - 4:20 PM EDT

 **LexisNexis**® [About LexisNexis](#) | [Terms & Conditions](#) | [Contact Us](#)  
Copyright © 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

18 Pa.C.S. § 5712

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS (R)

[Case Notes](#)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

Resources & Practice Tools

Treatises and Analytical Materials

> 43 P.L.E., SEARCHES AND SEIZURES § 72, Pennsylvania Law Encyclopedia, SEARCHES AND SEIZURES, § 72. Interception of Wire, Electronic, or Oral Communication. Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5712 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5712. Issuance of order and effect

(a) AUTHORIZING ORDERS.-- Each order authorizing the interception of any wire, electronic or oral communication shall state the following:

- (1) The identity of the investigative or law enforcement officers or agency to whom the authority to intercept wire, electronic or oral communications is given and the name and official identity of the person who made the application.
- (2) The identity of, or a particular description of, the person, if known, whose communications are to be intercepted.
- (3) The character and location of the particular communication facilities as to which, or the particular place of the communication as to which, authority to intercept is granted.
- (4) A particular description of the type of the communication to be intercepted and a statement of the particular offense to which it relates.
- (5) 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.

(b) TIME LIMITS.-- No order entered under this section shall authorize the interception of any wire, electronic or oral communication for a period of time in excess of that necessary under the circumstances. Every order entered under this section shall require that such interception begin and terminate as soon as practicable and be conducted in such a manner as to minimize or eliminate the interception of such communications not otherwise subject to interception under this chapter by making reasonable efforts, whenever possible, to reduce the hours of interception authorized by said order. In the event the intercepted communication is in a code or foreign language and an expert in that code or foreign language is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. No order entered under this section shall authorize the interception of wire, electronic or oral communications for any period exceeding 30 days. The 30-day period begins on the day on which the investigative or law enforcement officers or agency first begins to conduct an interception under the order, or ten days after the order is entered, whichever is earlier. Extensions or renewals of such an order may be granted for additional periods of not more than 30 days each. No extension or renewal shall be granted unless an application for it is made in accordance with this section, and the judge makes the findings required by section 5710 (relating to grounds for entry of order).

(c) RESPONSIBILITY.-- The order shall require the Attorney General or the district attorney, or their designees, to be responsible for the supervision of the interception.

(d) PROGRESS REPORTS.-- Whenever an order authorizing an interception is entered, 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. The reports shall be made at such intervals as the judge may require.

(e) FINAL REPORT.-- Whenever an interception is authorized pursuant to this section, a complete written list of names of participants and evidence of offenses discovered, including those not stated in the application for order, shall be filed with the court as soon as practicable after the authorized interception is terminated.

(f) ASSISTANCE.-- An order authorizing the interception of a wire, electronic or oral communication shall, upon request of the applicant, direct that a provider of electronic communication service 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 is affording the person whose communications are to be intercepted. The obligation of a provider of electronic communication service under such an order may include, but is not limited to, installation of a pen register or trap and trace device and disclosure of a record or other information otherwise available under section 5743 (relating to requirements for governmental access), including conducting an in-progress trace during an interception, provided that such obligation of a provider of electronic communications service is technologically feasible. Any provider of electronic communication service furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing the facilities or assistance. The service provider shall be immune from civil and criminal liability for any assistance rendered to the applicant pursuant to this section.

(g) ENTRY BY LAW ENFORCEMENT OFFICERS.-- An order authorizing the interception of a wire, electronic or oral communication shall, if requested, authorize the entry of premises or facilities specified in subsection (a)(3), or premises necessary to obtain access to the premises or facilities specified in subsection (a)(3), by the law enforcement officers specified in subsection (a)(1), as often as necessary solely for the purposes of installing, maintaining or removing an electronic, mechanical or other device or devices provided that such entry is

18 Pa.C.S. § 5712

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

[Case Notes](#)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF  
THE 2009 REGULAR SESSION\*

Resources & Practice Tools

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT  
THROUGH ACT 36\*

Treatises and Analytical  
Materials

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

> 43 P.L.E., SEARCHES AND  
SEIZURES § 72, Pennsylvania Law  
Encyclopedia, SEARCHES AND  
SEIZURES, § 72. Interception of  
Wire, Electronic, or Oral  
Communication, Copyright 2007,  
Matthew Bender & Company, Inc.,  
a member of the LexisNexis Group.

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND  
DECENCY

CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5712 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013,  
unless extended by Statute.

§ 5712. Issuance of order and effect

(a) AUTHORIZING ORDERS.-- Each order authorizing the interception of any wire,  
electronic or oral communication shall state the following:

- (1) The identity of the investigative or law enforcement officers or agency to whom the authority to intercept wire, electronic or oral communications is given and the name and official identity of the person who made the application.
- (2) The identity of, or a particular description of, the person, if known, whose communications are to be intercepted.
- (3) The character and location of the particular communication facilities as to which, or the particular place of the communication as to which, authority to intercept is granted.
- (4) A particular description of the type of the communication to be intercepted and a statement of the particular offense to which it relates.
- (5) 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.

(b) **TIME LIMITS.**-- No order entered under this section shall authorize the interception of any wire, electronic or oral communication for a period of time in excess of that necessary under the circumstances. Every order entered under this section shall require that such interception begin and terminate as soon as practicable and be conducted in such a manner as to minimize or eliminate the interception of such communications not otherwise subject to interception under this chapter by making reasonable efforts, whenever possible, to reduce the hours of interception authorized by said order. In the event the intercepted communication is in a code or foreign language and an expert in that code or foreign language is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. No order entered under this section shall authorize the interception of wire, electronic or oral communications for any period exceeding 30 days. The 30-day period begins on the day on which the investigative or law enforcement officers or agency first begins to conduct an interception under the order, or ten days after the order is entered, whichever is earlier. Extensions or renewals of such an order may be granted for additional periods of not more than 30 days each. No extension or renewal shall be granted unless an application for it is made in accordance with this section, and the judge makes the findings required by section 5710 (relating to grounds for entry of order).

(c) **RESPONSIBILITY.**-- The order shall require the Attorney General or the district attorney, or their designees, to be responsible for the supervision of the interception.

(d) **PROGRESS REPORTS.**-- Whenever an order authorizing an interception is entered, 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. The reports shall be made at such intervals as the judge may require.

(e) **FINAL REPORT.**-- Whenever an interception is authorized pursuant to this section, a complete written list of names of participants and evidence of offenses discovered, including those not stated in the application for order, shall be filed with the court as soon as practicable after the authorized interception is terminated.

(f) **ASSISTANCE.**-- An order authorizing the interception of a wire, electronic or oral communication shall, upon request of the applicant, direct that a provider of electronic communication service 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 is affording the person whose communications are to be intercepted. The obligation of a provider of electronic communication service under such an order may include, but is not limited to, installation of a pen register or trap and trace device and disclosure of a record or other information otherwise available under section 5743 (relating to requirements for governmental access), including conducting an in-progress trace during an interception, provided that such obligation of a provider of electronic communications service is technologically feasible. Any provider of electronic communication service furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing the facilities or assistance. The service provider shall be immune from civil and criminal liability for any assistance rendered to the applicant pursuant to this section.

(g) **ENTRY BY LAW ENFORCEMENT OFFICERS.**-- An order authorizing the interception of a wire, electronic or oral communication shall, if requested, authorize the entry of premises or facilities specified in subsection (a)(3), or premises necessary to obtain access to the premises or facilities specified in subsection (a)(3), by the law enforcement officers specified in subsection (a)(1), as often as necessary solely for the purposes of installing, maintaining or removing an electronic, mechanical or other device or devices provided that such entry is

reasonably necessary to accomplish the purposes of this subchapter and provided that the judge who issues the order shall be notified of the time and method of each such entry prior to entry if practical and, in any case, within 48 hours of entry.

#### History:

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately; Act 1998-19 (S.B. 635), § 8, approved Feb. 18, 1998, eff. immediately..

LexisNexis (R) Notes:

#### Case Notes:



1. 18 Pa. Cons. Stat. § 5712(C) provides that the court shall require the attorney general or the district attorney, or their designees, to be responsible for the supervision of the interception of electronic eavesdropping. *Commonwealth v. Doty*, 345 Pa. Super. 374, 498 A.2d 870, 1985 Pa. Super. LEXIS 8324 (1985), writ of certiorari denied by 479 U.S. 853, 93 L. Ed. 2d 119, 107 S. Ct. 185, 1986 U.S. LEXIS 3877, 55 U.S.L.W. 3235 (1986).
2. Under 18 Pa. Cons. Stat. § 5712(B) electronic eavesdropping may not be authorized for a more time than is necessary under the circumstances, must begin and end as soon as practicable, and must be minimized by reasonable efforts whenever possible. *Commonwealth v. Doty*, 345 Pa. Super. 374, 498 A.2d 870, 1985 Pa. Super. LEXIS 8324 (1985), writ of certiorari denied by 479 U.S. 853, 93 L. Ed. 2d 119, 107 S. Ct. 185, 1986 U.S. LEXIS 3877, 55 U.S.L.W. 3235 (1986).
3. Final report regarding electronic eavesdropping is required by 18 Pa. Cons. Stat. § 5712 (E), and shall be filed with the court at the time the authorized surveillance is terminated. *Commonwealth v. Doty*, 345 Pa. Super. 374, 498 A.2d 870, 1985 Pa. Super. LEXIS 8324 (1985), writ of certiorari denied by 479 U.S. 853, 93 L. Ed. 2d 119, 107 S. Ct. 185, 1986 U.S. LEXIS 3877, 55 U.S.L.W. 3235 (1986).



4. Former 18 Pa. Cons. Stat. § 5721(a)(3) (repealed), provided for a motion to suppress the contents of an intercepted oral communication on the ground that the interception was not



18 Pa.C.S. § 5713

[Retrieve State Legislative Impact® \(\\$\)](#)

[Practitioner's Toolbox](#)



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*  
\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*  
\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5713 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5713. Emergency situations

(a) APPLICATION.-- Whenever, upon informal application by the Attorney General or a designated deputy attorney general authorized in writing by the Attorney General or a district attorney or an assistant district attorney authorized in writing by the district attorney of a county wherein the suspected criminal activity has been, is or is about to occur, a judge determines there are grounds upon which an order could be issued pursuant to this chapter, and that an emergency situation exists with respect to the investigation of an offense designated in section 5708 (relating to order authorizing interception of wire, electronic or oral communications), and involving conspiratorial activities characteristic of organized crime or a substantial danger to life or limb, dictating authorization for immediate interception of wire, electronic or oral communications before an application for an order could with due diligence be submitted to him and acted upon, the judge may grant oral approval for such interception without an order, conditioned upon the filing with him, within 48 hours thereafter, of an application for an order which, if granted, shall recite the oral approval and be retroactive to the time of such oral approval. Such interception shall immediately terminate when the communication sought is obtained or when the application for an order is denied, whichever is earlier. In the event no application for an order is made, the content of any wire, electronic or oral communication intercepted shall be treated as having been obtained in violation of this subchapter.

(b) FURTHER PROCEEDINGS.-- In the event no application is made or an application made pursuant to this section is denied, the court shall cause an inventory to be served as provided in section 5716 (relating to service of inventory and inspection of intercepted communications) and shall require the tape or other recording of the intercepted communication to be delivered to, and sealed by, the court. Such evidence shall be retained by the court in accordance with section 5714 (relating to recording of intercepted

communications) and the same shall not be used or disclosed in any legal proceeding except in a civil action brought by an aggrieved person pursuant to section 5725 (relating to civil action for unlawful interception, disclosure or use of wire, electronic or oral communication) or as otherwise authorized by court order. In addition to other remedies and penalties provided by this chapter, failure to effect delivery of any such tape or other recording shall be punishable as contempt by the court directing such delivery. Evidence of oral authorization to intercept wire, electronic or oral communications shall be a defense to any charge against the investigating or law enforcement officer for engaging in unlawful interception.

#### **History:**

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately; Act 1998-19 (S.B. 635), § 9, approved Feb. 18, 1998, eff. immediately; Act 2002-162 (H.B. 976), § 4, approved Dec. 9, 2002, eff. in 60 days..

Source: [Legal](#) > / . . . / > **PA - Pennsylvania Statutes, Annotated by LexisNexis** 

View: Full

Date/Time: Tuesday, October 27, 2009 - 4:22 PM EDT



[About LexisNexis](#) | [Terms & Conditions](#) | [Contact Us](#)  
[Copyright ©](#) 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

18 Pa.C.S. § 5713.1

[Retrieve State Legislative Impact® \(\\$\)](#)

[Practitioner's Toolbox](#)



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*  
\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*  
\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5713.1 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5713.1. Emergency hostage and barricade situations

(a) DESIGNATION.-- The Attorney General or a district attorney may designate supervising law enforcement officers for the purpose of authorizing the interception of wire or oral communications as provided in this section.

(b) PROCEDURE.-- A supervising law enforcement officer who reasonably determines that an emergency situation exists that requires a wire or oral communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and who determines that there are grounds upon which an order could be entered under this chapter to authorize such interception, may intercept such wire or oral communication. An application for an order approving the interception must be made by the supervising law enforcement officer in accordance with section 5709 (relating to application for order) within 48 hours after the interception has occurred or begins to occur. Interceptions pursuant to this section shall be conducted in accordance with the procedures of this subchapter. Upon request of the supervising law enforcement officer who determines to authorize interceptions of wire communications under this section, a provider of electronic communication service shall provide assistance and be compensated therefor as provided in section 5712(f) (relating to issuance of order and effect). In the absence of an order, such interception shall immediately terminate when the situation giving rise to the hostage or barricade situation ends or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied or in any other case where the interception is terminated without an order having been issued, the contents of any wire or oral communication intercepted shall be treated as having been obtained in violation of this subchapter, and an inventory shall be served as provided in section 5716 (relating to service of inventory and inspection of intercepted communications). Thereafter, the supervising law enforcement officer shall follow the procedures set forth in section 5713(b) (relating to emergency situations).

(c) DEFENSE.-- A good faith reliance on the provisions of this section shall be a complete defense to any civil or criminal action brought under this subchapter or any other statute against any law enforcement officer or agency conducting any interceptions pursuant to this section as well as a provider of electronic communication service who is required to provide assistance in conducting such interceptions upon request of a supervising law enforcement officer.

(d) DEFINITIONS.-- As used in this section, the following words and phrases shall have the meanings given to them in this subsection:

"EMERGENCY SITUATION." Any situation where:

- (1) a person is holding a hostage and is threatening serious physical injury will resist with the use of weapons; or
- (2) a person has barricaded himself and taken a position of confinement to avoid apprehension and:
  - (i) has threatened to resist with the use of weapons; or
  - (ii) is threatening suicide or harm to others.

"SUPERVISING LAW ENFORCEMENT OFFICER."

- (1) For designations by a district attorney, any law enforcement officer trained pursuant to section 5724 (relating to training) to carry out interceptions under this section who has attained the rank of lieutenant or higher in a law enforcement agency within the county or who is in charge of a county law enforcement agency; or
- (2) For designations by the Attorney General, any member of the Pennsylvania State Police trained pursuant to section 5724 to carry out interceptions under this section and designated by the Commissioner of the Pennsylvania State Police who:
  - (i) has attained the rank of lieutenant or higher; or
  - (ii) is in charge of a Pennsylvania State Police barracks.

#### History:

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately; Act 1998-19 (S.B. 635), § 9, approved Feb. 18, 1998, eff. immediately..


Source: [Legal](#) > / . . . / > PA - Pennsylvania Statutes, Annotated by LexisNexis 

View: Full

Date/Time: Tuesday, October 27, 2009 - 4:23 PM EDT

18 Pa.C.S. § 5714

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox 

PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS (R)

 [Case Notes](#)

 [History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*

Resources & Practice Tools

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*

Treatises and Analytical Materials

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

> 43 P.L.E., SEARCHES AND SEIZURES § 72, Pennsylvania Law Encyclopedia, SEARCHES AND SEIZURES, § 72. Interception of Wire, Electronic, or Oral Communication, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5714 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5714. Recording of intercepted communications

(a) RECORDING AND MONITORING.-- Any wire, electronic or oral communication intercepted in accordance with this subchapter shall, if practicable, be recorded by tape or other comparable method. The recording shall be done in such a way as will protect it from editing or other alteration. Whenever an interception is being monitored, the monitor shall be an investigative or law enforcement officer certified under section 5724 (relating to training), and where practicable, keep a signed, written record which shall include the following:

- (1) The date and hours of surveillance.
- (2) The time and duration of each intercepted communication.
- (3) The participant, if known, in each intercepted conversation.
- (4) A summary of the content of each intercepted communication.

(b) SEALING OF RECORDINGS.-- Immediately upon the expiration of the order or extensions or renewals thereof, all monitor's records, tapes and other recordings shall be transferred to the judge issuing the order and sealed under his direction. Custody of the tapes, or other recordings shall be maintained wherever the court directs. They shall not be destroyed except upon an order of the court and in any event shall be kept for ten years. Duplicate tapes, or other recordings may be made for disclosure or use pursuant to section 5717 (relating to investigative disclosure or use of contents of wire, electronic or oral

communications or derivative evidence). The presence of the seal provided by this section, or a satisfactory explanation for its absence, shall be a prerequisite for the disclosure of the contents of any wire, electronic or oral communication, or evidence derived therefrom, under section 5717(b).


#### History:

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately; Act 1998-19 (S.B. 635), § 9, approved Feb. 18, 1998, eff. immediately..

LexisNexis (R) Notes:

#### Case Notes:



 1. Contents of a wire communication were held to be under seal under 18 Pa. Cons. Stat. § 5714, however possession of the communication was not illegal, only the disclosure of the contents under seal. *Boettger v. Loverro*, 521 Pa. 366, 555 A.2d 1234, 1989 Pa. LEXIS 74, 16 Media L. Rep. (BNA) 1467 (1989), vacated by 493 U.S. 885, 107 L. Ed. 2d 178, 110 S. Ct. 225, 1989 U.S. LEXIS 4828, 58 U.S.L.W. 3239 (1989).



2. Threatening phone conversations that were made by defendants and recorded by the recipient, an accomplice and witness for the commonwealth in defendants' trial for robbery and criminal conspiracy, were properly admitted in evidence and did not violate the Wiretapping and Electronic Surveillance Control Act, specifically 18 Pa. Cons. Stat. § 5714(a) because: (1) the recordings were consensual as to the accomplice, (2) they were sufficiently protected from alteration or editing, and (3) the logging was adequate. *Commonwealth v. Whiting*, 447 Pa. Super. 35, 668 A.2d 151, 1995 Pa. Super. LEXIS 3373 (1995), appeal denied by 544 Pa. 629, 675 A.2d 1247, 1996 Pa. LEXIS 630 (1996), appeal denied sub nomine *Commonwealth v. Cooke*, 544 Pa. 653, 676 A.2d 1195, 1996 Pa. LEXIS 961 (1996).

#### Treatises and Analytical Materials:

1. 43 P.L.E., SEARCHES AND SEIZURES § 72, Pennsylvania Law Encyclopedia, SEARCHES AND SEIZURES, § 72. Interception of Wire, Electronic, or Oral Communication, Copyright

18 Pa.C.S. § 5715

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS (R)

[Case Notes](#)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

Resources & Practice Tools

Law Reviews

> 13 Widener L.J. 11, SYMPOSIUM: WHEN A LAWYER STOOD TALL: SHARING AND UNDERSTANDING STORIES OF LAWYER HEROES: The Ascent of an Ancient Palladium: The Resurgent Importance of Trial by Jury and the Coming Revolution in Pennsylvania Sentencing.

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5715 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5715. Sealing of applications, orders and supporting papers

Applications made, final reports, and orders granted pursuant to this subchapter and supporting papers and monitor's records shall be sealed by the court and shall be held in custody as the court shall direct and shall not be destroyed except on order of the court and in any event shall be kept for ten years. They may be disclosed only upon a showing of good cause before a court of competent jurisdiction except that any investigative or law enforcement officer may disclose such applications, orders and supporting papers and monitor's records to investigative or law enforcement officers of this or another state, any of its political subdivisions, or of the United States to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure. In addition to any remedies and penalties provided by this subchapter, any violation of the provisions of this section may be punished as contempt of the court.

**History:**

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately; Act 1998-19 (S.B. 635), § 9, approved Feb. 18, 1998, eff. immediately..

18 Pa.C.S. § 5715

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox 

PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

 [Case Notes](#)

 [History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF  
THE 2009 REGULAR SESSION\*

Resources & Practice Tools

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT  
THROUGH ACT 36\*

Law Reviews

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

> 13 Widener L.J. 11, SYMPOSIUM:  
WHEN A LAWYER STOOD TALL:  
SHARING AND UNDERSTANDING  
STORIES OF LAWYER HEROES: The  
Ascent of an Ancient Palladium: The  
Resurgent Importance of Trial by  
Jury and the Coming Revolution in  
Pennsylvania Sentencing.

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND  
DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5715 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013,  
unless extended by Statute.

§ 5715. Sealing of applications, orders and supporting papers

Applications made, final reports, and orders granted pursuant to this subchapter and supporting papers and monitor's records shall be sealed by the court and shall be held in custody as the court shall direct and shall not be destroyed except on order of the court and in any event shall be kept for ten years. They may be disclosed only upon a showing of good cause before a court of competent jurisdiction except that any investigative or law enforcement officer may disclose such applications, orders and supporting papers and monitor's records to investigative or law enforcement officers of this or another state, any of its political subdivisions, or of the United States to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure. In addition to any remedies and penalties provided by this subchapter, any violation of the provisions of this section may be punished as contempt of the court.

 **History:**

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately; Act 1998-19 (S.B. 635), § 9, approved Feb. 18, 1998, eff. immediately..



18 Pa.C.S. § 5716

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

[Case Notes](#)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF  
THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*  
\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5716 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5716. Service of inventory and inspection of intercepted communications

(a) SERVICE OF INVENTORY.-- Within a reasonable time but not later than 90 days after the termination of the period of the order or of extensions or renewals thereof, or the date of the denial of an order applied for under section 5713 (relating to emergency situations) or 5713.1 (relating to emergency hostage and barricade situations), the issuing or denying judge shall cause to be served on the persons named in the order, application, or final report an inventory which shall include the following:

- (1) Notice of the entry of the order or the application for an order denied under section 5713 or 5713.1.
- (2) The date of the entry of the order or the denial of an order applied for under section 5713 or 5713.1.
- (3) The period of authorized or disapproved interception.
- (4) The fact that during the period wire or oral communications were or were not intercepted.

(b) POSTPONEMENT.-- On an ex parte showing of good cause to the issuing or denying judge the service of the inventory required by this section may be postponed for a period of 30 days. Additional postponements may be granted for periods of not more than 30 days on an ex parte showing of good cause to the issuing or denying judge.

(c) INSPECTIONS.-- The court, upon the filing of a motion, shall make available to such

persons or their attorneys for inspection, the intercepted communications and monitor's records to which the movant was a participant and the applications and orders.

**History:**

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately.

LexisNexis (R) Notes:

**Case Notes:**

1. In addition to a final report of electronic eavesdropping, 18 Pa. Cons. Stat. § 5716 provides that the court shall cause an inventory to be filed not later than 90 days after the termination of the period of the order or of extensions or renewals thereof. Commonwealth v. Doty, 345 Pa. Super. 374, 498 A.2d 870, 1985 Pa. Super. LEXIS 8324 (1985), writ of certiorari denied by 479 U.S. 853, 93 L. Ed. 2d 119, 107 S. Ct. 185, 1986 U.S. LEXIS 3877, 55 U.S.L.W. 3235 (1986).

Source: [Legal](#) > / . . . / > **PA - Pennsylvania Statutes, Annotated by LexisNexis**

View: Full

Date/Time: Tuesday, October 27, 2009 - 4:26 PM EDT



[About LexisNexis](#) | [Terms & Conditions](#) | [Contact Us](#)

Copyright © 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

18 Pa.C.S. § 5717

[Retrieve State Legislative Impact® \(\\$\)](#)

PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF  
THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT  
THROUGH ACT 36\*

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND  
DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC  
SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL  
COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5717 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will  
expire on December 31, 2013, unless extended by Statute.

§ 5717. Investigative disclosure or use of contents of wire, electronic or oral communications  
or derivative evidence

(a) LAW ENFORCEMENT PERSONNEL. --Any investigative or law enforcement officer who,  
under subsection (a.1) or (b), has obtained knowledge of the contents of any wire, electronic  
or oral communication, or evidence derived therefrom, may disclose such contents or  
evidence 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.

(A.1) USE OF INFORMATION.-- Any investigative or law enforcement officer who, by any  
means authorized by this subchapter, has obtained knowledge of the contents of any wire,  
electronic or oral communication or evidence derived therefrom may use such contents or  
evidence to the extent such use is appropriate to the proper performance of his official  
duties.

(b) EVIDENCE.-- Any person who by any means authorized by this chapter, has obtained  
knowledge of the contents of any wire, electronic or oral communication, or evidence derived  
therefrom, may disclose such contents or evidence to an investigative or law enforcement  
officer and may disclose such contents or evidence while giving testimony under oath or  
affirmation in any criminal proceeding in any court of this Commonwealth or of another state  
or of the United States or before any state or Federal grand jury or investigating grand jury.

Practitioner's Toolbox



[Case Notes](#)

[Opinions of Attorney General](#)

[History](#)

Resources & Practice Tools

Treatises and Analytical  
Materials

- > 24 P.L.E., EVIDENCE § 61, Pennsylvania Law Encyclopedia, EVIDENCE, § 61. Telephone Conversations, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.
- > 43 P.L.E., SEARCHES AND SEIZURES § 72, Pennsylvania Law Encyclopedia, SEARCHES AND SEIZURES, § 72. Interception of Wire, Electronic, or Oral Communication, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.
- > 48 P.L.E., TELECOMMUNICATIONS § 3, Pennsylvania Law Encyclopedia, TELECOMMUNICATIONS, § 3. ----- Disclosure or Publication, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

18 Pa.C.S. § 5718

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox

PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS (R)

[Case Notes](#)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
 TITLE 18. CRIMES AND OFFENSES  
 PART II. DEFINITION OF SPECIFIC OFFENSES  
 ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
 CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
 SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

Resources & Practice Tools

Treatises and Analytical Materials

- > 43 P.L.E., SEARCHES AND SEIZURES § 72, Pennsylvania Law Encyclopedia, SEARCHES AND SEIZURES, § 72. Interception of Wire, Electronic, or Oral Communication, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.
- > 48 P.L.E., TELECOMMUNICATIONS § 2, Pennsylvania Law Encyclopedia, TELECOMMUNICATIONS, § 2. -- Intercepting Communications, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5718 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5718. Interception of communications relating to other offenses

When an investigative or law enforcement officer, while engaged in court authorized interceptions of wire, electronic or oral communications in the manner authorized herein, intercepts wire, electronic or oral communications relating to offenses other than those specified in the order of authorization, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in section 5717(a) (relating to investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence). Such contents and evidence may be disclosed in testimony under oath or affirmation in any criminal proceeding in any court of this Commonwealth or of another state or of the United States or before any state or Federal grand jury when authorized by a judge who finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this subchapter. Such application shall be made as soon as practicable.

**History:**

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately; Act 1998-19 (S.B. 635), § 9, approved Feb. 18, 1998, eff. immediately..

18 Pa.C.S. § 5719

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

[Case Notes](#)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF  
THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5719 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5719. Unlawful use or disclosure of existence of order concerning intercepted communication

Except as specifically authorized pursuant to this subchapter any person who willfully uses or discloses the existence of an order authorizing interception of a wire, electronic or oral communication is guilty of a misdemeanor of the second degree.

**History:**

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately; Act 1998-19 (S.B. 635), § 9, approved Feb. 18, 1998, eff. immediately..

LexisNexis (R) Notes:

**Case Notes:**

18 Pa.C.S. § 5720

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

[Case Notes](#)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF  
THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5720 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5720. Service of copy of order and application before disclosure of intercepted communication in trial, hearing or proceeding

The contents of any wire, electronic or oral communication intercepted in accordance with the provisions of this subchapter, or evidence derived therefrom, shall not be disclosed in any trial, hearing, or other adversary proceeding before any court of the Commonwealth unless, not less than ten days before the trial, hearing or proceeding the parties to the action have been served with a copy of the order, the accompanying application and the final report under which the interception was authorized or, in the case of an interception under section 5704 (relating to exceptions to prohibition of interception and disclosure of communications), notice of the fact and nature of the interception. The service of inventory, order, application, and final report required by this section may be waived by the court only where it finds that the service is not feasible and that the parties will not be prejudiced by the failure to make the service.

**History:**

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately; Act 1998-19 (S.B. 635), § 9, approved Feb. 18, 1998, eff. immediately..

**NOTES:**

18 Pa.C.S. § 5721

[Retrieve State Legislative Impact® \(\\$\)](#)

PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS (R)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5721 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

This section is suspended in part where inconsistent with Pa.R.J.C.P. No 340, pursuant to Pa.R.J.C.P. No. 800, for purposes of delinquency proceedings.

§ 5721. Repealed. 1998, Feb. 18, P.L. 102, No. 19, imd. effective

LexisNexis (R) Notes:

**🔍 Law Reviews:**

1. 33 Duq. L. Rev. 361, Recent Decision: Constitutional Law--Criminal Procedure--Child Testimony Via Videotape or Closed Circuit Television--Defendant's Right To Confront Witnesses--The Supreme Court of Pennsylvania held that a statute allowing children to testify outside the physical presence of a defendant by means of videotape or closed circuit television violates the defendant's constitutional right to confront witnesses face-to-face. The court further held that Article I, section 9 of the Pennsylvania Constitution requires a face-to-face confrontation between a defendant and a witness, and allows exceptions only when the defendant has previously had the opportunity to physically confront and crossexamine the witness., Winter, 1995.

2. 33 Duq. L. Rev. 523, RECENT DEVELOPMENT: Recent Developments in Pennsylvania Law \*, Spring, 1995.

**Practitioner's Toolbox**



**Resources & Practice Tools**

**Law Reviews**

- > 33 Duq. L. Rev. 361, Recent Decision: Constitutional Law--Criminal Procedure--Child Testimony Via Videotape or Closed Circuit Television--Defendant's Right To Confront Witnesses--The Supreme Court of Pennsylvania held that a statute allowing children to testify outside the physical presence of a defendant by means of videotape or closed circuit television violates the defendant's constitutional right to confront witnesses face-to-face. The court further held that Article I, section 9 of the Pennsylvania Constitution requires a face-to-face confrontation between a defendant and a witness, and allows exceptions only when the defendant has previously had the opportunity to physically confront and crossexamine the witness., Winter, 1995.
- > 33 Duq. L. Rev. 523, RECENT DEVELOPMENT: Recent Developments in Pennsylvania Law \*, Spring, 1995.

18 Pa.C.S. § 5721.1

[Retrieve State Legislative Impact® \(\\$\)](#)

PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF  
THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT  
THROUGH ACT 36\*

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND  
DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC  
SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL  
COMMUNICATION

[Go to the Pennsylvania Code Archive Directory](#)

18 Pa.C.S. § 5721.1 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5721.1. Evidentiary disclosure of contents of intercepted communication or derivative evidence

(a) DISCLOSURE IN EVIDENCE GENERALLY.--

(1) Except as provided in paragraph (2), no person shall disclose the contents of any wire, electronic or oral communication, or evidence derived therefrom, in any proceeding in any court, board or agency of this Commonwealth.

(2) Any person who has obtained knowledge of the contents of any wire, electronic or oral communication, or evidence derived therefrom, which is properly subject to disclosure under section 5717 (relating to investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence), may also disclose such contents or evidence in any matter relating to any criminal, quasi-criminal, forfeiture, administrative enforcement or professional disciplinary proceedings in any court, board or agency of this Commonwealth or of another state or of the United States or before any state or Federal grand jury or investigating grand jury. Once such disclosure has been made, then any person may disclose the contents or evidence in any such proceeding.

Practitioner's Toolbox

[Case Notes](#)

[History](#)

Resources & Practice Tools

Treatises and Analytical  
Materials

- > 43 P.L.E., SEARCHES AND SEIZURES § 72, Pennsylvania Law Encyclopedia, SEARCHES AND SEIZURES, § 72. Interception of Wire, Electronic, or Oral Communication, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.
- > 48 P.L.E., TELECOMMUNICATIONS § 2, Pennsylvania Law Encyclopedia, TELECOMMUNICATIONS, § 2. -- Intercepting Communications, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

[More...](#)



(3) Notwithstanding the provisions of paragraph (2), no disclosure in any such proceeding shall be made so long as any order excluding such contents or evidence pursuant to the provisions of subsection (b) is in effect.

(b) MOTION TO EXCLUDE.-- Any aggrieved person who is a party to any proceeding in any court, board or agency of this Commonwealth may move to exclude the contents of any wire, electronic or oral communication, or evidence derived therefrom, on any of the following grounds:

(1) Unless intercepted pursuant to an exception set forth in section 5704 (relating to exceptions to prohibition of interception and disclosure of communications), the interception was made without prior procurement of an order of authorization under section 5712 (relating to issuance of order and effect) or an order of approval under section 5713(a) (relating to emergency situations) or 5713.1(b) (relating to emergency hostage and barricade situations).

(2) The order of authorization issued under section 5712 or the order of approval issued under section 5713(a) or 5713.1(b) was not supported by probable cause with respect to the matters set forth in section 5710(a)(1) and (2) (relating to grounds for entry of order).

(3) The order of authorization issued under section 5712 is materially insufficient on its face.

(4) The interception materially deviated from the requirements of the order of authorization.

(5) With respect to interceptions pursuant to section 5704(2), the consent to the interception was coerced by the Commonwealth.

(6) Where required pursuant to section 5704(2)(iv), the interception was made without prior procurement of a court order, or without probable cause.

(c) PROCEDURE.--

(1) The motion shall be made in accordance with the applicable rules of procedure governing such proceedings. The court, board or agency, upon the filing of such motion, shall make available to the movant or his counsel the intercepted communication and evidence derived therefrom.

(2) In considering a motion to exclude under subsection (b)(2), both the written application under section 5710(a) and all matters that were presented to the judge under section 5710(b) shall be admissible.

(3) The movant shall bear the burden of proving by a preponderance of the evidence the grounds for exclusion asserted under subsection (b)(3) and (4).

(4) With respect to exclusion claims under subsection (b)(1), (2) and (5), the respondent shall bear the burden of proof by a preponderance of the evidence.

(5) With respect to exclusion claims under subsection (b)(6), the movant shall have the initial burden of demonstrating by a preponderance of the evidence that the interception took place in his home. Once he meets this burden, the burden shall shift to the respondent to demonstrate by a preponderance of the evidence that the interception was in accordance with section 5704(2)(iv).

(6) Evidence shall not be deemed to have been derived from communications excludable under subsection (b) if the respondent can demonstrate by a preponderance of the evidence that the Commonwealth or the respondent had a basis independent of the excluded communication for discovering such evidence, or that such evidence would have been inevitably discovered by the Commonwealth or the respondent absent the excluded communication.

(d) APPEAL.-- In addition to any other right of appeal, the Commonwealth shall have the right to appeal from an order granting a motion to exclude if the official to whom the order authorizing the intercept was granted shall certify to the court that the appeal is not taken for purposes of delay. The appeal shall be taken in accordance with the provisions of Title 42 (relating to judiciary and judicial procedure).

(e) EXCLUSIVENESS OF REMEDIES AND SANCTIONS.-- The remedies and sanctions described in this subchapter with respect to the interception of wire, electronic or oral communications are the only judicial remedies and sanctions for nonconstitutional violations of this subchapter involving such communications.

**History:**

Act 1998-19 (S.B. 635), § 11, approved Feb. 18, 1998, eff. immediately.

LexisNexis (R) Notes:

**Case Notes:**



1. Tape recording an alleged sexual assault victim made of a phone conversation with



\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*  
\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*  
\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5722 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5722. Report by issuing or denying judge

Within 30 days after the expiration of an order or an extension or renewal thereof entered under this subchapter or the denial of an order confirming verbal approval of interception, the issuing or denying judge shall make a report to the Administrative Office of Pennsylvania Courts stating the following:

- (1) That an order, extension or renewal was applied for.
- (2) The kind of order applied for.
- (3) That the order was granted as applied for, was modified, or was denied.
- (4) The period of the interceptions authorized by the order, and the number and duration of any extensions or renewals of the order.
- (5) The offense specified in the order, or extension or renewal of an order.
- (6) The name and official identity of the person making the application and of the investigative or law enforcement officer and agency for whom it was made.
- (7) The character of the facilities from which or the place where the communications were to be intercepted.

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*  
\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*  
\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5723 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5723. Annual reports and records of Attorney General and district attorneys

(a) JUDGES.-- In addition to reports required to be made by applicants pursuant to Title 18 U.S.C. § 2519, all judges who have issued orders pursuant to this title shall make annual reports on the operation of this chapter to the Administrative Office of Pennsylvania Courts. The reports by the judges shall contain the following information:

- (1) The number of applications made.
- (2) The number of orders issued.
- (3) The effective periods of such orders.
- (4) The number and duration of any renewals thereof.
- (5) The crimes in connection with which the orders were sought.
- (6) The names and official identity of the applicants.
- (7) Such other and further particulars as the Administrative Office of Pennsylvania Courts may require.

(b) ATTORNEY GENERAL.-- In addition to reports required to be made by applicants pursuant to Title 18 U.S.C. § 2519, the Attorney General shall make annual reports on the operation of this chapter to the Administrative Office of Pennsylvania Courts and to the Judiciary Committees of the Senate and House of Representatives. The reports by the Attorney General shall contain the same information which must be reported pursuant to 18

U.S.C. § 2519(2).

(c) DISTRICT ATTORNEYS.-- Each district attorney shall annually provide to the Attorney General all of the foregoing information with respect to all applications authorized by that district attorney on forms prescribed by the Attorney General.

(d) OTHER REPORTS.-- The Chief Justice of the Supreme Court and the Attorney General shall annually report to the Governor and the General Assembly on such aspects of the operation of this chapter as they deem appropriate and make any recommendations they feel desirable as to legislative changes or improvements to effectuate the purposes of this chapter and to assure and protect individual rights.

🚩 **History:**

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately.

Source: [Legal](#) > / . . . / > PA - Pennsylvania Statutes, Annotated by LexisNexis 

View: Full

Date/Time: Tuesday, October 27, 2009 - 4:30 PM EDT



[About LexisNexis](#) | [Terms & Conditions](#) | [Contact Us](#)

[Copyright](#) © 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

18 Pa.C.S. § 5724

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS  
(R)

[Case Notes](#)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF  
THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*  
\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5724 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5724. Training

The Attorney General and the Commissioner of the Pennsylvania State Police shall establish a course of training in the legal and technical aspects of wiretapping and electronic surveillance as allowed or permitted by this subchapter, shall establish such regulations as they find necessary and proper for such training program and shall establish minimum standards for certification and periodic recertification of Commonwealth investigative or law enforcement officers as eligible to conduct wiretapping or electronic surveillance under this chapter. The Pennsylvania State Police shall charge each investigative or law enforcement officer who enrolls in this training program a reasonable enrollment fee to offset the costs of such training.

**History:**

Act 1988-115 (S.B. 797), § 5, approved Oct. 21, 1988, eff. immediately; Act 1998-19 (S.B. 635), § 12, approved Feb. 18, 1998, eff. immediately..

**NOTES:**

PENNSYLVANIA ADMINISTRATIVE CODE REFERENCES.

1. 37 Pa. Code Part I, Ch 51 (2009), PART STATE POLICE.

18 Pa.C.S. § 5725

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS (R)

[Case Notes](#)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

Resources & Practice Tools

Treatises and Analytical Materials

- > 10 P.L.E., CONSTITUTIONAL LAW § 132, Pennsylvania Law Encyclopedia, CONSTITUTIONAL LAW, § 132. Freedom of Speech and of the Press, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.
- > 48 P.L.E., TELECOMMUNICATIONS § 1, Pennsylvania Law Encyclopedia, TELECOMMUNICATIONS, § 1. Offenses Generally, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.
- > 48 P.L.E., TELECOMMUNICATIONS § 2, Pennsylvania Law Encyclopedia, TELECOMMUNICATIONS, § 2. -- Intercepting Communications, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5725 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

[More...](#)

§ 5725. Civil action for unlawful interception, disclosure or use of wire, electronic or oral communication

(a) CAUSE OF ACTION.-- Any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication; and shall be entitled to recover from any such person:

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

(2) Punitive damages.

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

(b) WAIVER OF SOVEREIGN IMMUNITY.-- To the extent that the Commonwealth and any of its officers, officials or employees would be shielded from liability under this section by the doctrine of sovereign immunity, such immunity is hereby waived for the purposes of this section.





18 Pa.C.S. § 5726

[Retrieve State Legislative Impact® \(\\$\)](#)

Practitioner's Toolbox



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS (R)

[Case Notes](#)

Resources & Practice Tools

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*

\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*

\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

Treatises and Analytical Materials

> 40 P.L.E., PUBLIC OFFICERS AND EMPLOYEES § 41, Pennsylvania Law Encyclopedia, PUBLIC OFFICERS AND EMPLOYEES, § 41. In General, Copyright 2007, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5726 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5726. Action for removal from office or employment

(a) CAUSE OF ACTION. --Any aggrieved person shall have the right to bring an action in Commonwealth Court against any investigative or law enforcement officer, public official or public employee seeking the officer's, official's or employee's removal from office or employment on the grounds that the officer, official or employee has intentionally violated the provisions of this chapter. If the court shall conclude that such officer, official or employee has in fact intentionally violated the provisions of this chapter, the court shall order the dismissal or removal from office of said officer, official or employee.

(b) DEFENSE. --It is a defense to an action brought pursuant to subsection (a) that the actor acted in good faith reliance on a court order or the provisions of this chapter.

LexisNexis (R) Notes:

**Case Notes:**



18 Pa.C.S. § 5727

Retrieve State Legislative Impact® (\$)

PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS(R)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*  
\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*  
\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5727 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5727. Repealed. 1988, Oct. 21, P.L. 1000, No. 115, § 6, imd. effective.

Source: [Legal](#) > / . . . / > PA - Pennsylvania Statutes, Annotated by LexisNexis 

View: Full

Date/Time: Tuesday, October 27, 2009 - 4:33 PM EDT



LexisNexis®

[About LexisNexis](#) | [Terms & Conditions](#) | [Contact Us](#)

[Copyright ©](#) 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

18 Pa.C.S. § 5727

Retrieve State Legislative Impact® (\$)

PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS(R)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*  
\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*  
\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5727 (2009)

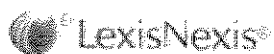
NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5727. Repealed. 1988, Oct. 21, P.L. 1000, No. 115, § 6, imd. effective.

Source: [Legal](#) > / . . . / > **PA - Pennsylvania Statutes, Annotated by LexisNexis**

View: Full

Date/Time: Tuesday, October 27, 2009 - 4:33 PM EDT



[About LexisNexis](#) | [Terms & Conditions](#) | [Contact Us](#)

[Copyright ©](#) 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

18 Pa.C.S. § 5728

[Retrieve State Legislative Impact® \(\\$\)](#)

[Practitioner's Toolbox](#)



PENNSYLVANIA STATUTES, ANNOTATED BY LEXISNEXIS(R)

[History](#)

\*THIS DOCUMENT IS CURRENT THROUGH THE ACT 21 OF THE 2009 REGULAR SESSION\*  
\*EXCEPT FOR TITLES 43 THRU 45 WHICH ARE CURRENT THROUGH ACT 36\*  
\*\*\* OCTOBER 9, 2009 ANNOTATION SERVICE \*\*\*

PENNSYLVANIA CONSOLIDATED STATUTES  
TITLE 18. CRIMES AND OFFENSES  
PART II. DEFINITION OF SPECIFIC OFFENSES  
ARTICLE F. OFFENSES AGAINST PUBLIC ORDER AND DECENCY  
CHAPTER 57. WIRETAPPING AND ELECTRONIC SURVEILLANCE  
SUBCHAPTER B. WIRE, ELECTRONIC OR ORAL COMMUNICATION

**Go to the Pennsylvania Code Archive Directory**

18 Pa.C.S. § 5728 (2009)

NOTICE: Pursuant to 18 Pa.C.S. § 5781, this Chapter will expire on December 31, 2013, unless extended by Statute.

§ 5728. 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 subchapter, the Attorney General may initiate a civil action in the Commonwealth Court to enjoin the violation. The court shall proceed as soon as practicable to the hearing and determination of the action and may, at any time before final determination, enter a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the Commonwealth or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Pennsylvania Rules of Civil Procedure, except that, if a criminal complaint has been filed against the respondent, discovery is governed by the Pennsylvania Rules of Criminal Procedure.

**History:**

Act 1988-115 (S.B. 797), § 7, approved Oct. 21, 1988, eff. immediately.

Source: [Legal](#) > / . . . / > PA - Pennsylvania Statutes, Annotated by LexisNexis

View: Full

Date/Time: Tuesday, October 27, 2009 - 4:35 PM EDT



LexisNexis

[About LexisNexis](#) | [Terms & Conditions](#) | [Contact Us](#)

Copyright © 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

FOCUS™ Terms 781 A.2d 85

Search Within Original Results (1 - 551)

Advanced...

Form: [All Guided Search Forms](#) > [Cases](#)Terms: [name\(White\)](#) ([Edit Search](#) | [Suggest Terms for My Search](#))Focus: [781 A.2d 85](#) ([Exit FOCUS™](#))

344 N.J. Super. 211, \*; 781 A.2d 85, \*\*;  
2001 N.J. Super. LEXIS 370, \*\*\*

WILLIAM WHITE, PLAINTIFF, v. MARY WHITE, DEFENDANT.

DOCKET NO. FM-20-00567-00

SUPERIOR COURT OF NEW JERSEY, CHANCERY DIVISION-FAMILY PART, UNION COUNTY

344 N.J. Super. 211; **781 A.2d 85**; 2001 N.J. Super. LEXIS 370

May 31, 2001, Decided

**SUBSEQUENT HISTORY:** [\*\*\*1] APPROVED FOR PUBLICATION September 26, 2001.**CASE SUMMARY**

**PROCEDURAL POSTURE:** In a contested custody matter, plaintiff husband moved to suppress, on grounds of violation of the New Jersey Wiretap Act, [N.J. Stat. Ann. §§ 2A:156A-1](#) to -34, and common law violation of privacy, his stored e-mails retrieved by defendant wife from the hard drive of the family computer.

**OVERVIEW:** While a couple's divorce was pending, the husband continued to live in the sunroom of the marital home. All family members had access to the room, where the family computer and home entertainment center were located. After discovering evidence of the husband's infidelity, the wife and her investigator retrieved e-mail messages between the husband and his girlfriend, and the court held that these could be introduced in evidence if they were relevant to its custody determination. The wife had not violated the New Jersey Wiretap Act, [N.J. Stat. Ann. §§ 2A:156A-1](#) to -34, because she was an authorized user of the computer and the messages could not have been intercepted if they were already in post-transmission storage. She also had not invaded the husband's privacy, because he could not possibly have had an expectation of privacy in the sunroom, under the circumstances of the family's living arrangement.

**OUTCOME:** The court denied the motion to suppress.

**CORE TERMS:** storage, e-mail, electronic communications, user, privacy, drive, electronic, message, transmission, intrusion, password, authorization, stored, recipient, mail, expectation of privacy, post-transmission, wiretap, spouse, Wiretap Act, technology, accessed, cabinet, intermediate, wiretapping, accessing, intercept, invasion, attachment, server

**LEXISNEXIS® HEADNOTES**

Hide

[Communications Law](#) > [Privacy](#) > [Wiretap Acts](#)

[Computer & Internet Law](#) > [Criminal Offenses](#) > [General Overview](#)

[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Miscellaneous Offenses](#) > [General Overview](#)

HN1 The New Jersey Wiretap Act, [N.J. Stat. Ann. §§ 2A:156A-1](#) to -34, applies when one spouse illegally records the communications of the other spouse. [More Like This Headnote](#)

[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Miscellaneous Offenses](#) > [Illegal Eavesdropping](#) > [General Overview](#)

HN2 It is not the function of the courts to graft an exemption where the legislature has not seen fit to provide one. [More Like This Headnote](#)

[Communications Law](#) > [Privacy](#) > [Wiretap Acts](#)

[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Miscellaneous Offenses](#) > [Illegal Eavesdropping](#) > [General Overview](#)

[Evidence](#) > [Illegal Eavesdropping](#) > [Wiretaps](#)


HN3 The New Jersey Wiretap Act, [N.J. Stat. Ann. §§ 2A:156A-1](#) to -34, applies to unauthorized access of electronic communications of one's spouse. [More Like This Headnote](#) | [Shepardize: Restrict By Headnote](#)

[Computer & Internet Law](#) > [Privacy & Security](#) > [Invasion of Privacy](#)


[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Miscellaneous Offenses](#) > [General Overview](#)

HN4 See [N.J. Stat. Ann. § 2A:156A-27\(a\)](#).


[Computer & Internet Law](#) > [Privacy & Security](#) > [Invasion of Privacy](#) 

[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Miscellaneous Offenses](#) > [General Overview](#) 

**HN5** ✚ See [N.J. Stat. Ann. § 2A:156A-1\(g\)](#).

[Computer & Internet Law](#) > [Privacy & Security](#) > [Electronic Communications Privacy Act](#) 


[Computer & Internet Law](#) > [Privacy & Security](#) > [Invasion of Privacy](#) 

[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Miscellaneous Offenses](#) > [Illegal Eavesdropping](#) > [General Overview](#) 

**HN6** ✚ The New Jersey Wiretap Act, [N.J. Stat. Ann. §§ 2A:156A-1 to -34](#), is not meant to extend to e-mail retrieved by the recipient and then stored. It protects only those electronic communications which are in the course of transmission or are backup to that course of transmission. [More Like This Headnote](#) | [Shepardize: Restrict By Headnote](#)


[Computer & Internet Law](#) > [Privacy & Security](#) > [Invasion of Privacy](#) 

[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Fraud](#) > [Computer Fraud](#) > [General Overview](#) 

[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Miscellaneous Offenses](#) > [General Overview](#) 

**HN7** ✚ Within the context of [N.J. Stat. Ann. § 2A:156A-27\(a\)](#), "without authorization" means using a computer from which one has been prohibited, or using another's password or code without permission. Where a party consents to another's access to its computer network, it cannot claim that such access was unauthorized. [More Like This Headnote](#)


[Computer & Internet Law](#) > [Privacy & Security](#) > [Invasion of Privacy](#) 

[Criminal Law & Procedure](#) > [Criminal Offenses](#) > [Miscellaneous Offenses](#) > [Illegal Eavesdropping](#) > [General Overview](#) 

**HN8** ✚ For purposes of the prohibition on interceptions, as defined by [N.J. Stat. Ann. § 2A:156A-3\(a\)](#), of e-mail, an electronic communication, by definition, cannot be intercepted when it is in electronic storage, because only communications can be intercepted, and the electronic storage of an electronic communication is by definition not part of the communication. [More Like This Headnote](#) | [Shepardize: Restrict By Headnote](#)

[Computer & Internet Law](#) > [Privacy & Security](#) > [Invasion of Privacy](#) 

[Torts](#) > [Intentional Torts](#) > [Defamation](#)


[Torts](#) > [Intentional Torts](#) > [Invasion of Privacy](#) > [Intrusion](#) > [Elements](#) 

**HN9** ✚ The common law recognizes various causes of action relating to the right to privacy. [More Like This Headnote](#)

[Torts](#) > [Intentional Torts](#) > [Invasion of Privacy](#) > [Intrusion](#) > [Elements](#) 

**HN10** ✚ One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for the invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself or it may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, by searching his safe or his wallet, by examining his private bank account, or by compelling him by a forged court order to permit an inspection of his personal documents. The intrusion itself makes the defendant subject to liability, even though there is no publication. [More Like This Headnote](#) | [Shepardize: Restrict By Headnote](#)

[Criminal Law & Procedure](#) > [Search & Seizure](#) > [Expectation of Privacy](#) 

[Torts](#) > [Intentional Torts](#) > [Invasion of Privacy](#) > [Intrusion](#) > [General Overview](#) 

**HN11** ✚ To be actionable, an intrusion must be highly offensive to a reasonable person, and that conclusion turns on one's reasonable expectation of privacy. A reasonable person cannot conclude that an intrusion is highly offensive when the actor intrudes into an area in which the victim has either a limited or no expectation of privacy. Expectations of privacy are established by general social norms. And, using a Fourth Amendment analysis for purposes of analogy, one's expectation of privacy must be reasonable--objectively reasonable. A person's expectation of privacy regarding a room used for storage and to which others have keys and access is not reasonable, and a subjective belief that the room is private is irrelevant. [More Like This Headnote](#) | [Shepardize: Restrict By Headnote](#)

**COUNSEL:** Robert S. Raymar for plaintiff, (*Helling Lindeman Goldstein & Siegal LLP*).

Phyllis Klein O'Brien for defendant, (*Donahue, Braun, Hagan, Klein & Newsome*).

**JUDGES:** ISSENMAN, J.S.C.

**OPINION BY:** ISSENMAN, J.S.C.

## OPINION

[\*214] [\*\*86] ISSENMAN, J.S.C.

## I INTRODUCTION

This opinion supplements an oral opinion rendered on April 23, 2001.

In this bitterly contested custody matter, the court is required to decide whether or not the defendant wife, by retrieving plaintiff husband's stored e-mail from the hard drive of the family computer, unlawfully accessed stored electronic communications, in violation of the New Jersey Wiretap Act, [N.J.S.A. 2A:156A-1 to 34](#) [the "Act"], or violated plaintiff's common [\*\*87] law right to privacy. Plaintiff [\*215] seeks to suppress the evidence if the Act was violated or if his privacy was wrongfully invaded.

No New Jersey court has yet interpreted the Act, or examined the tort issue, in the context of recent electronic communication technology. Because this court holds that the Act does not apply to the electronic communications stored under these circumstances [\*\*\*2] and there is no violation of the Act, and because this court also holds there is no invasion of plaintiff's right to privacy, the evidence will not be suppressed.

## II FACTS

The parties were married on April 26, 1980, and three children were born of their marriage: Ryan, 19; Colin 15; and Patrick, 13. Although plaintiff filed for divorce in October 1999, he continues to reside with defendant. He sleeps in the sun room.

The family computer and entertainment center are located in the sun room. The defendant and the children often use this room to utilize the computer, watch television, and adjust the stereo volume. It is also the only way to get to the grill out on the deck. It was in this room that defendant discovered a letter from plaintiff to his girlfriend. According to defendant, this letter was left in plain view; plaintiff denies this.

Shortly after defendant discovered the letter, she hired Gamma Investigative Research, and unbeknownst to plaintiff--and without using plaintiff's password--Gamma copied plaintiff's files from the computer's hard drive. These files contained e-mail sent between plaintiff and his girlfriend; they also contained images that he viewed on Netscape. [\*\*\*3] Gamma then prepared a written report detailing its findings and sent copies of all the above to defendant and her attorney. It was only while being deposed that plaintiff learned that defendant had accessed his e-mail. He had thought--incorrectly as it turns out--that his e-mail and attachments could not be read without his AOL password.

[\*216] In order to understand the error of plaintiff's thinking, it is necessary to first understand the technical workings of America Online Service ["AOL"], plaintiff's chosen Internet Service Provider ["ISP"]. Defendant's expert, John Passerini, explains it as follows:

Incoming e-mails are received on the AOL e-mail server and are accessible to an AOL user only after dialing in and authenticating with the user's screen name and password. Also, a user cannot send an e-mail via the AOL server until he has similarly dialed in . . . .

AOL's server receives and maintains the e-mail until the recipient dials into AOL and accesses (seeks to read) his mail.

In addition, an AOL user can save his e-mails and attachments on his computer's hard drive. AOL offers the Personal Filing Cabinet ["PFC"] feature, which is created automatically on the [\*\*\*4] hard drive during the installation of AOL on the user's computer. The PFC is named for user's screen name . . . .

[A]n AOL user must voluntarily choose to save the e-mail, attachment or address to his PFC or address book. The AOL user can save e-mail, attachments, or addresses either by using the automatic AOL feature or manually. To save automatically to the PFC on the hard drive, the user must select that option in "Mail Preferences." Specifically, in the main tool bar, the user chooses "Mail Center," "Preferences" and then checks "Retain All Mail I Send in My Personal Filing Cabinet" and/or [\*\*88] "Retain All Mail I Read in My Personal Filing Cabinet"

. . . .

Additionally, in the "Notes" section of [the Help screens], America On Line informs the user that he can read mail stored in the PFC when he is not signed onto AOL, i.e. the PFC is on the hard drive. Similarly . . . America On Line informs the user that e-mail saved in the PFC will remain on the hard drive until the user deletes it.

Mr. Passerini states that the only way to be sure "that e-mail will be saved permanently, is to use the PFC file on the user's hard drive . . ." because, "e-mail cannot be saved permanently on AOL's server. [\*\*\*5] "

It is clear that plaintiff was saving his e-mails--received and sent--to the PFC of the family computer. It is also clear that he did not realize he was doing so. Obviously, not knowing they were being saved, he took no steps to delete them, nor any steps to protect them with a password--a task easily accomplished.

As Mr. Passerini states:

[T]he PFC file on the user's hard drive is not automatically password protected . . . . While the AOL sign-on password is mandatory and required by AOL to establish a dial-up connection, *if no PFC password is created, any computer user [\*217] may view a PFC and e-mails contained in a PFC by simply opening the AOL software on the hard drive.* (emphasis added)

This is precisely what occurred here: defendant's expert simply opened the AOL software on the family computer's hard drive and viewed and copied plaintiff's e-mails.

Finally, it should be noted that as the result of the parties' entering into a protective order, this court has no knowledge of the contents of the e-mails which are the subject matter of this motion. Suffice it to say, defendant believes that they are highly relevant and material to the custody determination yet to [\*\*\*6] be made.

## III ANALYSIS

### A. Inter-Spousal Immunity

The first issue to be decided is whether or not the New Jersey Wiretap Act applies to a spouse who accesses the electronic communication of their spouse without authorization. It is already settled law <sup>HN1</sup> that the Act applies when one spouse illegally records the communications of the other spouse. Scott v. Scott, 277 N.J. Super. 601, 649 A.2d 1372 (Ch.Div.1994); M.G. v. J.C., 254 N.J. Super. 470, 603 A.2d 990 (Ch.Div.1991).

As the M.G. court stated:

It is clear that the language of the N.J. Wiretapping Act contains no explicit exemption for any wiretapping by an aggrieved spouse. <sup>HN2</sup> It is not the function of the courts to graft an exemption where the legislature has not seen fit to provide one.

[Id. at 477, 603 A.2d 990.]

The M.G. logic applicable to spousal wiretapping is equally applicable to spousal electronic communications. The legislature has amended the Act several times since M.G. v. J.C. and Scott v. Scott were decided. P.L. 1993 C. 29; P.L. 1994 C. 55; and P.L. 1999 C. 151. If the legislature did not see fit to enact a spousal exemption <sup>\*\*\*7</sup> when it amended the Act, it is not this court's function to do so. This court therefore concludes that <sup>HN3</sup> the New Jersey Wiretap Act applies to unauthorized access of electronic communications **[\*218]** of one's spouse, even though there was no violation of the Act in this case.

### B. The Wiretap Statute

The New Jersey Wiretapping and Electronic Surveillance Control Act, N.J.S.A. **[\*\*89]** 2A:156A-1 et seq., was enacted in 1968. It is identical to the Federal Wiretap Act. 18 U.S.C. § 2510 et seq.; See M.G. v. J.C., supra, 254 N.J. Super. at 473, 603 A.2d 990.

Congress enacted the Act in 1968 to protect wire and oral communications from being intercepted. New Jersey quickly followed suit. Since then, both the Congress and state legislatures "have been trying to keep pace with technology, while struggling with the question of what protection certain devices deserve." Vanessa Winter, Note, *What Is a Private Communication: An Analysis of the New Jersey Wiretap Act*, 19 *Seton Hall Leg. J.* 386 (1994).

In 1986, Congress amended the Federal Wiretap Act by enacting the Electronic Communications Privacy Act of 1986 [hereinafter <sup>\*\*\*8</sup> ECPA]. The purpose was to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." *Senate Report No. 99-541*, 99th Cong., 2d Sess. 1 (1986) [hereinafter *Senate Report*].

In enacting the ECPA, Congress recognized that "computers are used extensively today for the storage and processing of information," *Id.* at 3, and that while a first class letter was "afforded a high level of protection against unauthorized opening," there were "no comparable . . . statutory standards to protect the privacy and security of communications" transmitted by "new forms of telecommunications and computer technology." *Id.* at 5. And so, adopting the Electronic Communications Privacy Act of 1986 represented a "fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies." *Ibid.*

**[\*219]** New Jersey amended its wiretap act in 1993. P.L. 1993, C. 29. These amendments, regulating access of stored electronic communications, were identical to the amendments made to the Federal Wiretap statute by the ECPA. See Cacciarelli v. Boniface, 325 N.J. Super. 133, 136, 737 A.2d 1170 (Ch.Div.1999). <sup>\*\*\*9</sup>

The New Jersey statute, as amended, provides:

<sup>HN4</sup>

A person is guilty of a crime of the fourth degree if he

- (1) knowingly accesses without authorization a facility through which an electronic communication service is provided or exceeds an authorization to access that facility, and
- (2) thereby obtains, alters, or prevents authorized access to a wire or electronic communication while the communication is in electronic storage.

[N.J.S.A. 2A:156A-27(a).]

At first blush, it would appear that accessing electronic communications in electronic storage without authorization is a violation of the Act. But, electronic storage as used in the Act means:

<sup>HN5</sup> (1) Any temporary, immediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and



(2) Any storage of such communication by an electronic communication service for purpose of backup protection of the communication . . .

[N.J.S.A. 2A:156A-1(g).]

To understand the import of this language, a basic understanding of how e-mail communication works is essential. As Judge Brody explained in *Fraser v. Nationwide Mutual Insurance Co.* [\*\*\*10] :

Transmission of e-mail from the sender to the recipient through an electronic communication system is indirect. First, an individual authorized to use the system logs on to the system to send a message. After a message is sent, the system stores the message in temporary [\*\*\*90] or intermediate storage. I will refer to this storage as "intermediate storage". After a message is sent, the system also stores a copy of the message in a separate storage for back-up protection, in the event that the system crashes before transmission is completed. I will refer to this storage as "back-up protection storage". In the course of transmission from the sender to the recipient, a message passes through both intermediate and back-up protection storage.

Transmission is completed when the recipient logs on to the system and retrieves the message from intermediate storage. After the message is retrieved by the intended recipient, the message is copied to a third type of storage, which I will call "post-transmission storage". A message may remain in post-transmission storage for several years.

[135 F.Supp.2d 623, 633-34, 2001 WL 290656, 7-8 (E.D.Pa.2001.) (Citations omitted).]

[\*220] In other [\*\*\*11] words, all e-mail is stored at some point in the transmission process. David J. Loundy, *E-Law 4: Computer Information Systems Law and System Operators Liability*, 21 *Seattle U.L.Rev.* 1075, 1145 (1998).

To be clear, the e-mail in the hard-drive of the White family computer accessed by defendant was in post-transmission storage. Referring back to the statutory language which defines electronic <sup>HN6</sup> storage, the Act was not meant to extend to e-mail retrieved by the recipient and then stored. It protects only those electronic communications which are in the course of transmission or are backup to that course of transmission. *Fraser v. Nationwide Mutual Ins. Co.*, *supra*, at 637.

The conclusion that the Act does not apply to electronic communications received by the recipient, placed in post-transmission storage, and then accessed by another without authorization, appears to make sense, when one considers that the "strong expectation of privacy with respect to communication in the course of transmission significantly diminishes once transmission is complete." *Fraser v. Nationwide Mutual Ins. Co.*, *supra*. And, also, it should [\*\*\*12] be noted that while Congress was concerned with the protection of an individual's privacy interests against unjustified intrusions in the original wiretap act, it did not attempt to deal with all such intrusions. See *United U.S. v. Turk*, 526 F.2d 654, 658-59 (5th Cir.1976), *cert. denied*, 429 U.S. 823, 97 S.Ct. 74, 50 L.Ed.2d 84 (1976). The language contained in the ECPA and in the New Jersey statute represents the "fair balance" between privacy expectations and legitimate intrusion that Congress and the New Jersey legislature attempted to achieve in trying to keep pace with the advances in technology.

Two last points: (1) defendant did not access plaintiff's e-mail "without authorization" in violation of N.J.S.A. 2A:156A-27(a); and (2) defendant's actions do not constitute an "intercept" as defined by N.J.S.A. 2A:156A-3(a).

[\*221] <sup>HN7</sup> It has been held that "without authorization" means using a computer from which one has been prohibited, or using another's password or code without permission. *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F.Supp.2d 817 (E.D.Mich.2000). Although she did [\*\*\*13] not often use the family computer, defendant had authority to do so. Additionally, defendant did not use plaintiff's password or code without authorization. Rather, she accessed the information in question by roaming in and out of different directories on the hard drive. As stated in *Sherman*, where a party "consents to another's access to its computer network, it cannot [\*\*\*91] claim that such access was unauthorized." *Id.* at 821.

As to the meaning of an "intercept," the treatment of messages in "electronic storage" is not governed by the restrictions on "interception." "Congress did not intend for 'intercept' to apply to 'electronic storage'". *Steve Jackson Games Inc. v. United States Secret Service*, 36 F.3d 457, 462 (5th Cir.1994).

Said another way,

<sup>HN8</sup> An "electronic communication," by definition, cannot be "intercepted" when it is in "electronic storage," because only "communications" can be "intercepted," and, . . . the "electronic storage" of an "electronic communication" is by definition not part of the communication.

[Bohach v. City of Reno, 932 F.Supp. 1232, 1236 (D.Nev.1996).]

Here, the electronic communications [\*\*\*14] had already ceased being in "electronic storage" as defined by the Act. They were in post-transmission storage--therefore defendant did not intercept them.

Interestingly, the language of the Act refers to "access" rather than "disclosure" or "use," thus one court has held that a person

"can disclose or use with impunity the contents of an electronic communication unlawfully obtained from electronic storage." Wesley College v. Pitts, 974 F.Supp. 375, 389, (D.Del.1997), *aff'd*, o.b. 172 F.3d 861 (3rd Cir.1998). Therefore, because there is no prohibition regarding disclosure or use of the information defendant obtained from the family computer's hard drive, defendant cannot be barred from using it.

[\*222] Finally, plaintiff argues that defendant needed a warrant or court order before accessing and copying the contents of his e-mail. That argument is specious. It is specious because it misconstrues the statutory language. N.J.S.A. 2A:156A-29 deals with who may *compel* disclosure of an electronic communication. The answer is only a law enforcement agency and only if the agency has first obtained a warrant or a court order. [\*\*\*15] Not only is defendant not obligated to obtain a warrant but she is legally incapable of doing so.

### C. Invasion of Privacy

"<sup>HN9</sup>The common law recognizes various causes of action relating to the right to privacy." Hennessey v. Coastal Eagle Point Oil Co., 129 N.J. 81, 95, 609 A.2d 11(1992). Plaintiff alleges that by accessing his e-mail, defendant committed the tort of "intrusion on seclusion."

The Restatement (Second) of Torts, § 652B (1977) states:<sup>HN10</sup>

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for the invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

[*Id.* at 378.]

The invasion may be by "physical intrusion into a place in which the plaintiff has secluded himself" . . . or it may be

by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or by compelling him by a forged court order to permit an inspection of his personal documents. [\*\*\*16] The intrusion itself makes the defendant subject to liability, even though there is no publication.

[*Id.* at comment b. 378-79.]

The crux of the issue is that <sup>HN11</sup>the intrusion must be "highly offensive to a reasonable person." *Id.* And that conclusion turns on one's reasonable expectation [\*\*92] of privacy. A "reasonable person" cannot conclude that an intrusion is "highly offensive" when the actor intrudes into an area in which the victim has either a limited or no expectation of privacy.

[\*223] "[E]xpectations of privacy are established by general social norms." State v. Hempel, 120 N.J. 182, 200, 576 A.2d 793 (1990). And, using a Fourth Amendment analysis for purposes of analogy, one's expectation of privacy must be reasonable-objectively reasonable. State v. Brown, 282 N.J.Super. 538, 547, 660 A.2d 1221 (App.Div.) *certif. denied*, 143 N.J. 322, 670 A.2d 1064(1995). A person's expectation of privacy to a room used for storage and to which others have keys and access is not reasonable. Defendant's subjective belief that the room was private is "irrelevant". *Ibid.*

The same is true here. Plaintiff lived in the sun room of the marital [\*\*\*17] residence; the children and defendant were in and out of this room on a regular basis. The computer was in this room and the entire family had access to it and used it. Whatever plaintiff's subjective beliefs were as to his privacy, objectively, any expectation of privacy under these conditions is not reasonable. Indeed even subjectively, plaintiff knew his living accommodations were not private; he avers that he did not leave the letter to his girlfriend in plain view.

In DelPresto v. DelPresto, 97 N.J.Super. 446, 235 A.2d 240 (App.Div.1967), a case similar to the case at bar, defendant husband sought to suppress evidence of his extramarital affair that his wife found "in one of the office file cabinets in a room to which plaintiff [wife] had complete access." *Id.* at 454, 235 A.2d 240. The papers, consisting of love letters sent to the defendant by his paramour and a jewelry receipt for jewelry not given to his wife, had been left "in files to which she [wife] had a full freedom of entry." *Id.*

The Appellate Division overruled the trial court's suppression of this evidence, saying:

Having a legitimate reason for being in the files, plaintiff [\*\*\*18] had a right to seize evidence she believed indicated her husband was being unfaithful.

[*Id.* at 456, 235 A.2d 240.]

Can it be said that defendant's activities here are "highly intrusive?" Hennessey, supra. She was searching for *indicia* [\*224] that her husband was involved in an extramarital liaison--not an uncommon occurrence in the realm of human experience. Is rummaging through files in a computer hard drive any different than rummaging through files in an unlocked file cabinet, as in DelPresto, supra

Not really.







#### IV CONCLUSION

Accessing post-transmission stored e-mail, under these circumstances, does not violate the New Jersey Wiretap Act. Nor do defendant's actions intrude upon plaintiff's common law right to seclusion. Plaintiff's motion is denied.

Form: [All Guided Search Forms > Cases](#)  
Terms: [name\(White\)](#) ([Edit Search](#) | [Suggest Terms for My Search](#))  
Focus: **781 A.2d 85** ([Exit FOCUS™](#))  
View: Full

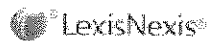
Date/Time: Monday, November 16, 2009 - 12:26 PM EST

\* Signal Legend:

-  - Warning: Negative treatment is indicated
-  - Questioned: Validity questioned by citing refs
-  - Caution: Possible negative treatment
-  - Positive treatment is indicated
-  - Citing Refs. With Analysis Available
-  - Citation information available

\* Click on any *Shepard's* signal to *Shepardize*® that case.

[My Lexis™](#) | [Search](#) | [Research Tasks](#) | [Get a Document](#) | [Shepard's®](#) | [Alerts](#) | [Total Litigator](#) | [Transactional Advisor](#) | [Counsel Selector](#)  
[History](#) | [Delivery Manager](#) | [Switch Client](#) | [Preferences](#) | [Sign Out](#) | [Help](#)



[About LexisNexis](#) | [Terms & Conditions](#) | [Contact Us](#)  
Copyright © 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

## Glossary of Terms

- ◆ **“Omnibus Crime Control and Safe Streets Act”**: enacted by Congress in 1968; Title III of the Act is the original federal Wiretap Act
- ◆ **“Electronic Communications Privacy Act (ECPA)”**: enacted by Congress in 1986 and divided into three sections; amended the Wiretap Act to include electronic communications (Title I); and added new legislation prohibiting unauthorized access to stored communications (Title II) and the use of pen/trap devices without a warrant (Title III)
- ◆ **“Wiretap Act”**: Title I of the ECPA; amended the former Wiretap Act to include electronic communications (such as e-mail)
- ◆ **“Stored Communications Act (SCA)”**: Title II of the ECPA; prohibits unauthorized access to stored wire and electronic communications
- ◆ **“Pen Register Act”**: Title III of the ECPA; created restrictions on private and law enforcement uses of pen registers and trap and trace devices
  - **“Pen register”**: an electronic device that records all numbers dialed from a particular telephone line (all outgoing numbers)
  - **“Trap and trace device”**: similar to a pen register, a trap and trace device records all numbers coming into a particular telephone line (all incoming numbers).
- ◆ **“Electronic communication”**: any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic or photooptical system
- ◆ **“Oral communication”**: face-to-face conversations where there is an expectation of privacy/non-interruption
- ◆ **“Wire communication”**: any aural transfer (transfer of the human voice) made through the use of facilities for the transmission of communications by the aid of wire, cable or other like connection (i.e., telephone and cellular phone conversations)
- ◆ **“Consent Rule”**: rule in federal and state wiretap statutes governing how many parties to a communication must consent in order for a wiretap to be lawful
  - **“One party consent”**: federal consent requirement in the ECPA and adopted by a majority of states; only one party to the conversation needs to consent to a wiretap for it to be lawful
  - **“Two/all party consent”**: a more stringent consent requirement adopted by a minority of states, PA included; requires consent from all parties to a

communication

- ◆ **“Electronic mail” (E-mail):** a method of electronic communication whereby an individual uses a computer or other electronic device to send and receive messages to/from other individuals; messages may be sent wirelessly or through computer systems linked to a network, through modems connected to telephone lines
  
- ◆ **“Intercept”:** 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
  
- ◆ **“Transmission” and “electronic storage”:** Transmission is the process of e-mail being transmitted from sender to recipient through an electronic communication system. Electronic storage is any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof, or any storage for purposes of backup protection of such communication. E-mail transmission involves the following electronic storage stages:
  - First, an individual authorized to use the system logs on to the system to send a message (e-mail). After a message is sent, the system stores the message in temporary or intermediate storage (**“mid-transmission storage”** or **“intermediate transmission storage”**).
  - After a message is sent, the system also stores a copy of the message in a separate storage for back-up protection, in the event that the system crashes before transmission is completed (**“back-up protection storage”**).
  - Transmission is completed when the recipient logs on to the system and retrieves the message from intermediate storage. After the message is retrieved by the intended recipient, the message is copied to a third type of storage, **“post-transmission storage.”** A message may remain in post-transmission storage for several years.<sup>1</sup>
  
- ◆ **“Hacking”:** refers to the process by which “hackers” gain unauthorized access to another’s computer; can also refer to the situation where one breaks into another’s e-mail without authorization

---

<sup>1</sup> This explanation of e-mail transmission storage is taken from *White v. White*, 344 N.J. Super. 211, 781 A.2d 85, 89-90 (Ch. Div. 2001) (citing Judge Brody’s explanation in *Fraser v. Nationwide Mutual Ins. Co.*, 135 F.Supp.2d 623, 633-634, 2001 WL 290656, 7-8 (E.D.Pa. 2001).

- ◆ **“Surveillance software”**: computer software that allows an individual to record a computer user’s activity, usually by “keystroke logging” or via “screenshots,” without the user knowing such activity is being recorded or monitored; the software usually saves this captured data in a log, which can later be retrieved by the installer, or it can e-mail the recorded data directly to the installer; popular surveillance software includes SpectorSoft, eBlaster, Visec, and e-Spy.
  - **“Keystroke logging”**: tracks the keys struck on a computer keyboard; can reveal a computer user’s activity (including passwords and access codes) by logging the user’s keystrokes
  - **“Screenshots”**: images captured by the computer which record the visible items on the monitor/screen of the computer in that instant; can reveal a computer user’s activity by snapping images of the programs, websites, instant messages and e-mails in use at a particular moment
    - ▶ **Popular surveillance software companies include:**
      - **SpectorSoft**
      - **eBlaster**
      - **e-Spy**
      - **Visec**
      - **SpyLab Inc.**