No. 1988-115

AN ACT

SB 797

Amending Title 18 (Crimes and Offenses) of the Pennsylvania Consolidated Statutes, limiting the defense of justification in certain cases; making an editorial change; providing for interception of certain communications and access to records pertaining thereto; providing for stored wire and communications and transactional records access, mobile tracking devices and pen registers and trap and trace devices; further providing for wiretapping and electronic surveillance; further providing for certain reports and penalties; and making a repeal.

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

Section 1. Section 509 of Title 18 of the Pennsylvania Consolidated Statutes is amended to read:

§ 509. Use of force by persons with special responsibility for care, discipline or safety of others.

The use of force upon or toward the person of another is justifiable if:

(1) The actor is the parent or guardian or other person similarly responsible for the general care and supervision of a minor or a person acting at the request of such parent, guardian or other responsible person and:

(i) the force is used for the purpose of safeguarding or promoting the welfare of the minor, including the preventing or punishment of his misconduct; and

(ii) the force used is not designed to cause or known to create a substantial risk of causing death, serious bodily injury, disfigurement, extreme pain or mental distress or gross degradation.

(2) The actor is a teacher or person otherwise entrusted with the care or supervision for a special purpose of a minor and:

(i) the actor believes that the force used is necessary to further such special purpose, including the maintenance of reasonable discipline in a school, class or other group, and that the use of such force is consistent with the welfare of the minor; and

(ii) the degree of force, if it had been used by the parent or guardian of the minor, would not be unjustifiable under **[subparagraph (1)(ii) of this section]** ***paragraph (1)(ii).***

(3) The actor is the guardian or other person similarly responsible for the general care and supervision of an incompetent, ***mentally ill or mentally retarded*** person; and:

(i) the force is used for the purpose of safeguarding or promoting the welfare of the incompetent, ***mentally ill or mentally retarded*** person, including the prevention of his misconduct, **[or, when such incompetent person is in a hospital or other institution for his care and custody, for**

the maintenance of reasonable discipline in such institution] ***and there is no reasonable alternative to the use of such force***; and

(ii) the force used is not designed to cause or known to create a substantial risk of causing death, **[serious]** bodily injury, disfigurement, **[extreme or]** unnecessary pain, mental distress, or humiliation.

(4) The actor is a doctor or other therapist or a person assisting him at his direction; and:

(i) the force is used for the purpose of administering a recognized form of treatment not prohibited by law of this Commonwealth which the actor believes to be adapted to promoting the physical or mental health of the patient; and

(ii) the treatment is administered with the consent of the patient, or, if the patient is a minor or an incompetent person with the consent of his parent or guardian or other person legally competent to consent in his behalf, or the treatment is administered in an emergency when the actor believes that no one competent to consent can be consulted and that a reasonable person, wishing to safeguard the welfare of the patient, would consent.

(5) The actor is a warden or other authorized official of a correctional institution; and:

(i) he believes that the force used is necessary for the purpose of enforcing the lawful rules or procedures of the institution, unless his belief in the lawfulness of the rule or procedure sought to be enforced is erroneous and his error is due to ignorance or mistake as to the provisions of this title, any other provision of the criminal law or the law governing the administration of the institution;

(ii) the nature or degree of force used is not forbidden by law; and

(iii) if deadly force is used, its use is otherwise justifiable under this chapter.

(6) The actor is a person responsible for the safety of a vessel or an aircraft or a person acting at his direction; and:

(i) he believes that the force used is necessary to prevent interference with the operation of the vessel or aircraft or obstruction of the execution of a lawful order, unless his belief in the lawfulness of the order is erroneous and his error is due to ignorance or mistake as to the law defining his authority; and

(ii) if deadly force is used, its use is otherwise justifiable under this chapter.

(7) The actor is a person who is authorized or required by law to maintain order or decorum in a vehicle, train or other carrier or in a place where others are assembled; and:

(i) he believes that the force used is necessary for such purpose; and

(ii) the force used is not designed to cause death, or known to create a substantial risk of causing death, bodily injury, or extreme mental distress.

Section 2. Chapter 57 of Title 18 is amended by adding a subchapter heading to read:

CHAPTER 57
WIRETAPPING AND ELECTRONIC SURVEILLANCE

SUBCHAPTER A
GENERAL PROVISIONS

Section 3. Section 5702 of Title 18 is amended to read:

§ 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 **[identity of the parties to such communication or the existence,]** 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) The radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit.

(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 an induction coil, 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.

"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.

"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.

["Intercepting device." Any device or apparatus, including an induction coil, that can be used to intercept a wire 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 communication common carrier in the ordinary course of its business, or purchased by any person, and being used by the subscriber, user, or person 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; or

(2) a hearing aid or similar device being used to correct sub-normal hearing to not better than normal.]

"Investigative or law enforcement officer." Any officer of the United States 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, and any attorney authorized by law to prosecute or participate in the prosecution of such offense. The term shall include, but not be limited to, employees of the Pennsylvania Crime Commission, authorized to investigate crimes enumerated in section 5708 (relating to order authorizing interception of wire or oral communications).

"Judge." **[As]** *When* referring to a judge authorized to receive applications for, and to enter, orders authorizing interceptions of wire **[and],** *electronic or* oral communications pursuant to this chapter, 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 **[communications]** *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 mechanical or electronic device which attaches to a particular telephone line, and which records outgoing numbers dialed by a *particular telephone, but does not:***

(1) monitor the contents of any communication; or

(2) record the origin of any incoming communications.]

A device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted, with respect to wire communications, on the telephone line to which the device is attached. 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.

"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 **[communications]** *communication.*" Any **[communication]** *aural transfer* made in whole or in part through the use of facilities for the transmission of **[communications]** *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 does not include the radio portion of a cordless telephone communication transmitted between the cordless telephone handset and the base unit.*

Section 4. Chapter 57 of Title 18 is amended by adding a subchapter heading to read:

SUBCHAPTER B
WIRE, ELECTRONIC OR ORAL COMMUNICATION

Section 5. Sections 5703, 5704, 5705, 5706, 5707, 5708, 5709, 5710, 5712, 5713, 5714, 5715, 5716, 5717, 5718, 5719, 5720, 5721, 5722, 5723, 5724 and 5725 of Title 18 are amended and the subchapter is amended by adding a section to read:

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

(2) **[willfully]** *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) **[willfully]** *intentionally* uses or endeavors to use the contents of any wire, *electronic* or oral **[communications]** *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.

§ 5704. Exceptions to prohibition **[on]** ***of*** interception and disclosure of communications.

It shall not be unlawful under this chapter for:

(1) An operator of a switchboard, or an officer, agent or employee of a **[communication common carrier]** ***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 **[carrier of such communication]** ***provider of wire or electronic communication service***. However, no **[communication common carrier]** ***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 where:

(i) such officer or person is a party to the communication; or

(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.

(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 **[communications]** *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 *or trap and trace device as provided in this chapter*.

(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. **[The]** *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 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.

§ 5705. Possession, sale, distribution, manufacture or advertisement of **[intercepting]** *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 **[intercepting]** *electronic, mechanical or other* devices), a person is guilty of a felony of the third degree if he does any of the following:

(1) **[Willfully]** ***Intentionally*** possesses an **[intercepting]** ***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) **[Willfully]** ***Intentionally*** sells, transfers or distributes an **[intercepting]** ***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) **[Willfully]** ***Intentionally*** manufactures or assembles an **[intercepting]** ***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) **[Willfully]** ***Intentionally*** places in any newspaper, magazine, handbill, or other publication any advertisement of **[any intercepting]** ***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 **[any intercepting]** ***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.

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

(a) Unlawful activities.—It shall not be unlawful under this chapter for:

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

(b) Responsibility.—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 **[intercepting]** ***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) ***and (12)*** (relating to exceptions to prohibition **[on]** ***of*** interception and disclosure of communications), 5712 (relating to issuance of order and effect) **[or]**, 5713 (relating to emergency situations) ***or 5713.1 (relating to emergency hostage and barricade situations). 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.***

§ 5707. Seizure and forfeiture of **[intercepting]** ***electronic, mechanical or other*** devices.

Any **[intercepting]** ***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.

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

(a) Authorization.—Except in cases referred to in subsection (b), 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 interception is to be made, 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 2706 (relating to terroristic threats)
Section 2901 (relating to kidnapping)
Section 3121 (relating to rape)
Section 3123 (relating to involuntary deviate sexual intercourse)
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)

(2) Under this title, where such offense is dangerous to life, limb or property and punishable by imprisonment for more than one year:
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 4108 (relating to commercial bribery and breach of duty to act disinterestedly)
Section 4109 (relating to rigging publicly exhibited contest)
Section 4902 (relating to perjury)
[Section 4907 (relating to tampering with witnesses and informants)]
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 5504 (relating to harassment by communication or address)
Section 5902 (relating to prostitution and related offenses)

(3) Under the act of **[July 22, 1970 (P.L.513, No.178), known as the "Pennsylvania Cigarette Tax Act,"]** ***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 902. Sales of unstamped cigarettes.
Section 903. Possession of unstamped cigarettes.
Section 904. Counterfeiting.]
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.

(b) Exception.—Whenever the interception of wire, ***electronic*** or oral communication is to be made by an investigative officer employed by the Pennsylvania Crime Commission, the application for the authorizing order shall be made by the Attorney General ***or, during the absence or incapacity of the Attorney General, a deputy attorney general designated in writing by the Attorney General.***

§ 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 interception is to be made 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 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 **[facilities]** ***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.

§ 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 **[a]** wire, ***electronic*** or oral **[communication]** ***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 **[communication is]** ***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 **[facilities]** ***facility*** from which, or the place where, the wire, ***electronic*** or oral communications are to be intercepted, **[are, have]** ***is, has*** been, or **[are]** ***is*** about to be used, in connection with the commission of such offense, or **[are]** ***is*** leased to, listed in the name of, or commonly used by, such **[individual]** ***person***;

(5) the investigative or law enforcement officers or agency to be authorized to intercept the wire, ***electronic*** or oral **[communication]** ***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.

§ 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 **[a]** wire, ***electronic*** or oral **[communication]** ***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. **[Except as provided in subsection (c), no]** ***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 **[20]** ***30*** days. **[An extension or renewal]** ***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 **[one]** additional **[period]** ***periods*** of not more than **[20 days]** ***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 **[a surveillance]** ***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 at the time the authorized **[surveillance]** ***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 **[communication common carrier]** ***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 **[carrier]** ***service provider*** is affording the person whose communications are to be intercepted. The obligation of a **[communication common carrier]** ***provider of electronic communication service*** under such an order may include but is not limited to conducting an in-progress trace during an interception. Any **[communication common carrier]** ***provider of electronic communication service*** furnishing such facilities or technical assistance shall be compensated **[therefore]** ***therefor*** by the applicant **[at the prevailing rates. Said carrier]** ***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 **[intercepting]** ***electronic, mechanical or other*** device or devices provided that such entry is reasonably necessary to accomplish the purposes of this chapter 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.

§ 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 interception is to be made, 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 **[and]** ***or*** a substantial danger to life or limb, dictating authorization for immediate interception of wire, ***electronic*** or oral **[com-**

munication] ***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 chapter.

(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 **[an oral or wire communication]** ***wire, electronic or oral communications*** shall be a defense to any charge against the investigating or law enforcement officer for engaging in unlawful interception.

§ 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 chapter. 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 chapter, 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 chapter 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.

(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.

§ 5714. Recording of intercepted communications.

(a) Recording and monitoring.—Any wire, *electronic* or oral communication intercepted in accordance with this chapter 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 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).

§ 5715. Sealing of applications, orders and supporting papers.

Applications made, final reports, and orders granted pursuant to this chapter 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 chapter, any violation of the provisions of this section may be punished as contempt of the court.

§ 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.

§ 5717. Disclosure or use of contents of wire, ***electronic*** or oral communications or derivative evidence.

(a) Investigative activities.—Any investigative or law enforcement officer 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 another investigative or law enforcement officer, ***including another investigative or law enforcement officer of another state or political subdivision thereof,*** or make use of such contents or evidence to the extent that such disclosure or use is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(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.

(c) Otherwise authorized personnel.—Any person who, by any means authorized by the laws of another state or the Federal Government, 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 where otherwise admissible while giving testimony under oath or affirmation in any proceeding in any court of this Commonwealth.

§ 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 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 **[in advance of such disclosure and on application to a court, the court finds that the contents were listed in the final report, pursuant to section 5712(e) (relating to issuance of order and effect), and]** ***authorized by a judge who 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.

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

Except as specifically authorized pursuant to this chapter 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.

§ 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 chapter, 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 **[on]** ***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.

§ 5721. Suppression of contents of intercepted communication or derivative evidence.

(a) Motion to suppress.—Any aggrieved person in any trial, hearing, or other adversary proceeding in or before any court or other authority of this Commonwealth may move to suppress the contents of any intercepted wire, ***electronic*** or oral communication, or evidence derived therefrom, on any of the following grounds:

(1) The communication was unlawfully intercepted.

(2) The order of authorization if required is insufficient on its face.

(3) The interception unless made in accordance with section 5704 (relating to exceptions to prohibition **[on]** ***of*** interception and disclosure of communications) was not made in conformity with the order of authorization or in accordance with the requirements of section 5712 (relating to issuance of order and effect).

(b) Procedure.—The motion shall be made at least ten days before the trial, hearing, or other adversary proceeding unless there was no opportunity to make the motion or the moving party was not aware of the grounds for the motion. Motions by co-indictees are to be heard in a single consolidated hearing. The court, upon the filing of such motion by the aggrieved person, shall make available to the aggrieved person or his counsel the intercepted

communication and evidence derived therefrom. If the motion is granted, the entire contents of all intercepted wire, ***electronic*** or oral communication obtained during or after any interception which is determined to be in violation of this chapter under subsection (a) or evidence derived therefrom, shall not be received in evidence in the trial, hearing or other adversary proceeding.

(c) Appeal.—In addition to any other right **[to]** ***of*** appeal, the Commonwealth shall have the right to appeal from an order granting a motion to suppress 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 (judiciary and judicial procedure).

(d) 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.

§ 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 chapter 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.

§ 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 **[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 conversations were sought.

(6) The names and official identity of the applicants.

(7) The number of indictments or informations resulting from each application.

(8) The crime or crimes which each indictment or information charges.

(9) The disposition of each indictment.] ***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.

§ 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 chapter***, 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.

§ 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 **[communications]** *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.

(c) 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.

Section 6. Section 5727 of Title 18 is repealed.

Section 7. Title 18 is amended by adding a section to read:

§ 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.

Section 8. Title 18 is amended by adding subchapters to read:

SUBCHAPTER C
STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

Sec.

5741. Unlawful access to stored communications.
5742. Disclosure of contents.
5743. Requirements for governmental access.
5744. Backup preservation.
5745. Delayed notice.
5746. Cost reimbursement.

5747. Civil action.
5748. Exclusivity of remedies.

§ 5741. Unlawful access to stored communications.

(a) Offense.—Except as provided in subsection (c), it is an offense to obtain, alter or prevent authorized access to a wire or electronic communication while it is in electronic storage by intentionally:

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

(2) exceeding the scope of one's authorization to access the facility.

(b) Penalty.—

(1) If the offense is committed for the purpose of commercial advantage, malicious destruction or damage, or private commercial gain, the offender shall be subject to:

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

(ii) a fine of not more than $250,000 or imprisonment for not more than two years, or both, for any subsequent offense.

(2) In any other case, the offender shall be subject to a fine of not more than $5,000 or imprisonment for not more than six months, or both.

(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 communication service;

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

(3) in section 5743 (relating to requirements for governmental access) or 5744 (relating to backup preservation).

§ 5742. Disclosure of contents.

(a) Prohibitions.—Except as provided in subsection (b):

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

(i) 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 the service.

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

(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:

(i) 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 the service.

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

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

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

(2) as otherwise authorized in section 5704(1) (relating to prohibition of interception and disclosure of communications), 5708 (relating to order authorizing interception of wire, electronic or oral communications) or 5743 (relating to governmental access);

(3) with the lawful consent of the originator or an addressee or intended recipient of the 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 the 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 the service; or

(6) to a law enforcement agency, if the contents:

(i) Were inadvertently obtained by the service provider.

(ii) Appear to pertain to the commission of a crime.

§ 5743. Requirements for governmental access.

(a) Contents of electronic communications in electronic storage.—Investigative or law enforcement officers may require the disclosure by a provider of electronic communication service of the contents of an electronic communication which is in electronic storage in an electronic communication system for:

(1) One hundred eighty days or less only pursuant to a warrant issued under the Pennsylvania Rules of Criminal Procedure.

(2) More than 180 days by the means available under subsection (b).

(b) Contents of electronic communications in a remote computing service.—

(1) Investigative or law enforcement officers may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2):

(i) without required notice to the subscriber or customer if the investigative or law enforcement officer obtains a warrant issued under the Pennsylvania Rules of Criminal Procedure; or

(ii) with prior notice from the investigative or law enforcement officer to the subscriber or customer if the investigative or law enforcement officer:

(A) uses an administrative subpoena authorized by a statute or a grand jury subpoena; or

(B) obtains a court order for the disclosure under subsection (d); except that delayed notice may be given pursuant to section 5745 (relating to delayed notice).

(2) Paragraph (1) is applicable with respect to an electronic communication which is held or maintained on that service:

(i) 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 the remote computing service.

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

(c) Records concerning electronic communication service or remote computing service.—

(1) Except as provided in paragraph (2), a provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of the service, not including the contents of communication covered by subsection (a) or (b), to any person other than an investigative or law enforcement officer.

(2) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of the service, not including the contents of communications covered by subsection (a) or (b), to an investigative or law enforcement officer only when the investigative or law enforcement officer:

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

(ii) obtains a warrant issued under the Pennsylvania Rules of Criminal Procedure;

(iii) obtains a court order for the disclosure under subsection (d); or

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

(3) An investigative or law enforcement officer receiving records or information under paragraph (2) is not required to provide notice to the customer or subscriber.

(d) Requirements for court order.—A court order for disclosure under subsection (b) or (c) shall be issued only if the investigative or law enforcement officer shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate investigative or law enforcement inquiry. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify the order if the information or records requested are unusually voluminous in nature or compliance with the order would otherwise cause an undue burden on the provider.

(e) No cause of action against a provider disclosing information under this chapter.—No cause of action shall lie against any provider of wire or

electronic communication service, its officers, employees, agents or other specified persons for providing information, facilities or assistance in accordance with the terms of a court order, warrant, subpoena or certification under this chapter.

§ 5744. Backup preservation.

(a) Backup preservation.—

(1) An investigative or law enforcement officer acting under section 5743(b)(2) (relating to requirements for governmental access) 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 the subpoena or court order, the service provider shall create the backup copy as soon as practicable, consistent with its regular business practices, and shall confirm to the investigative or law enforcement officer that the backup copy has been made. The 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 investigative or law enforcement officer within three days after receipt of confirmation that the backup copy has been made, unless the notice is delayed pursuant to section 5745(a) (relating to delayed notice).

(3) The service provider shall not destroy or permit the destruction of the backup copy until the later of:

(i) the delivery of the information; or

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

(4) The service provider shall release the backup copy to the requesting investigative or law enforcement officer no sooner than 14 days after the officer's notice to the subscriber or customer if the service provider has not:

(i) received notice from the subscriber or customer that the subscriber or customer has challenged the officer's request; and

(ii) initiated proceedings to challenge the request of the officer.

(5) An investigative or law enforcement officer may seek to require the creation of a backup copy under paragraph (1) if in his sole discretion the officer determines that there is reason to believe that notification under section 5743 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, customer or service provider.

(b) Customer challenges.—

(1) Within 14 days after notice by the investigative or law enforcement officer to the subscriber or customer under subsection (a)(2), the subscriber or customer may file a motion to quash the subpoena or vacate the court order, copies to be served upon the officer and written notice of the challenge to be given to the service provider. A motion to vacate a court order shall be filed in the court which issued the order. A motion to quash a subpoena shall be filed in the court which has authority to enforce the

subpoena. The motion or application shall contain an affidavit or sworn statement:

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

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

(2) Service shall be made under this section upon the investigative or law enforcement officer 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 Pennsylvania Rules of Civil Procedure.

(3) If the court finds that the customer has complied with paragraphs (1) and (2), the court shall order the investigative or law enforcement officer to file a sworn response, which may be filed in camera if the investigative or law enforcement officer 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 responses, 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 officer's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the investigative or law enforcement officer are maintained, or that there is reason to believe that the investigative or law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order the 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 reason to believe that the communications sought are relevant to a legitimate investigative or 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. The Commonwealth or investigative or law enforcement officer shall have the right to appeal from an order granting a motion or application under this section.

§ 5745. Delayed notice.

(a) Delay of notification.—

(1) An investigative or law enforcement officer acting under section 5743(b) (relating to requirements for governmental access) may:

(i) where a court order is sought, include in the application a request for an order delaying the notification required under section 5743(b) for a period not to exceed 90 days, which request the court shall grant if it 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); or

(ii) where an administrative subpoena authorized by a statute or a grand jury subpoena is obtained, delay the notification required under section 5743(b) for a period not to exceed 90 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).

(2) An adverse result for the purposes of paragraph (1) is:

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

(ii) flight from prosecution;

(iii) destruction of or tampering with evidence;

(iv) intimidation of potential witnesses; or

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

(3) The investigative or law enforcement officer shall maintain a true copy of a certification under paragraph (1)(ii).

(4) Extensions of the delay of notification provided for in section 5743 of up to 90 days each may be granted by the court upon application or by certification by a supervisory official in the case of an administrative or grand jury subpoena.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4), the investigative or law enforcement officer 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 which:

(i) states with reasonable specificity the nature of the investigative or law enforcement inquiry; and

(ii) informs the customer or subscriber:

(A) that information maintained for the customer or subscriber by the service provider named in the process or request was supplied to or requested by the investigative or law enforcement officer and the date on which the supplying or request took place;

(B) that notification of the customer or subscriber was delayed;

(C) the identity of the investigative or law enforcement officer or the court which made the certification or determination pursuant to which that delay was made; and

(D) which provision of this subchapter authorizes the delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent or assistant investigative agent in charge, or an equivalent, of an investigative or law enforcement 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.—An investigative or law enforcement officer acting under section 5743, when he is not required to notify the subscriber or customer under section 5743(b)(1), or to the extent that it may delay such notice pursuant to subsection (a), may apply to a court for an order commanding a provider of electronic communication service or remote computing service to whom a warrant, subpoena or court order is directed, not to notify any other person of the existence of the warrant, subpoena or court order for such period as the court deems appropriate. 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 a potential witness; or
(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

§ 5746. Cost reimbursement.

(a) Payment.—Except as otherwise provided in subsection (c), an investigative or law enforcement officer obtaining the contents of communications, records or other information under section 5742 (relating to disclosure of contents), 5743 (relating to requirements for governmental access) or 5744 (relating to backup preservation) shall reimburse the person or entity assembling or providing the information for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing and otherwise providing the information. Reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which the information may be stored.

(b) Amount.—The amount of the reimbursement provided for in subsection (a) shall be as mutually agreed upon by the investigative or law enforcement officer 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 the information or the court before which a criminal prosecution relating to the information would be brought, if no court order was issued for production of the information.

(c) Applicability.—The requirement of subsection (a) does not apply with respect to records or other information maintained by a communication common carrier which relates to telephone toll records and telephone listings obtained under section 5743. The court may, however, order reimbursement as described in subsection (a) if the court determines the information required is unusually voluminous or otherwise caused an undue burden on the provider.

§ 5747. Civil action.

(a) Cause of action.—Except as provided in subsection 5743(e) (relating to requirements for governmental access), any provider of electronic communication service, subscriber or customer aggrieved by any violation of this

subchapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in the 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) reasonable attorney fees and other litigation costs reasonably incurred.

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

(d) Defense.—A good faith reliance on:

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

(2) a request of an investigative or law enforcement officer under section 5713 (relating to emergency situations); or

(3) a good faith determination that section 5704(10) (relating to exceptions to prohibitions of interception and disclosure of communications) permitted the conduct complained of;

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

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

§ 5748. Exclusivity of remedies.

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

SUBCHAPTER D
MOBILE TRACKING DEVICES

Sec.
5761. Mobile tracking devices.

§ 5761. Mobile tracking devices.

(a) Authority to issue.—Orders for the installation and use of mobile tracking devices may be issued by a court of common pleas.

(b) Jurisdiction.—Orders permitted by this section may authorize the use of mobile tracking devices within the jurisdiction of the court of common pleas, and outside that jurisdiction but within this Commonwealth, if the device is installed within the jurisdiction of the court of common pleas.

(c) Standard for issuance of order.—An order authorizing the use of one or more mobile tracking devices may be issued to an investigative or law

enforcement officer by the court of common pleas upon written application. Each application shall be by written affidavit, signed and sworn to or affirmed before the court of common pleas. The affidavit shall:

(1) state the name and department, agency or address of the affiant;

(2) identify the vehicles, containers or items to which, in which or on which the mobile tracking device shall be attached or be placed, and the names of the owners or possessors of the vehicles, containers or items;

(3) state the jurisdictional area in which the vehicles, containers or items are expected to be found; and

(4) provide a statement setting forth all facts and circumstances which provide the applicant with a reasonable suspicion that criminal activity has been, is or will be in progress and that the use of a mobile tracking device will yield information relevant to the investigation of the criminal activity.

(d) Notice.—The court of common pleas shall be notified in writing within 72 hours of the time the mobile tracking device has been activated in place on or within the vehicles, containers or items.

(e) Term of authorization.—Authorization by the court of common pleas for the use of the mobile tracking device may continue for a period of 90 days from the placement of the device. An extension for an additional 90 days may be granted upon good cause shown.

(f) Removal of device.—Wherever practicable, the mobile tracking device shall be removed after the authorization period expires. If removal is not practicable, monitoring of the mobile tracking device shall cease at the expiration of the authorization order.

(g) Movement of device.—Movement of the tracking device within an area protected by a reasonable expectation of privacy shall not be monitored absent exigent circumstances or an order supported by probable cause that criminal activity has been, is or will be in progress in the protected area and that the use of a mobile tracking device in the protected area will yield information relevant to the investigation of the criminal activity.

SUBCHAPTER E
PEN REGISTERS AND TRAP AND TRACE DEVICES

Sec.

5771. General prohibition of pen register and trap and trace device use; exception.
5772. Application for an order for pen registers and trap and trace devices.
5773. Issuance of an order for a pen register or a trap and trace device.
5774. Assistance in installation and use of pen registers or trap and trace devices.
5775. Reports concerning pen registers.

§ 5771. General prohibition of pen register and trap and trace device use; exception.

(a) General rule.—Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 5773 (relating to issuance of an order for a pen register or a trap and trace device).

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

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

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

(c) Penalty.—Whoever intentionally and knowingly violates subsection (a) is guilty of a misdemeanor of the third degree.

§ 5772. Application for an order for pen registers and trap and trace devices.

(a) Application.—The Attorney General or a deputy attorney general designated in writing by the Attorney General or a district attorney or an assistant district attorney designated in writing by the district attorney may make application for an order or an extension of an order under section 5773 (relating to issuance of an order for a pen register or a trap and trace device) authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing, under oath or equivalent affirmation, to a court of common pleas.

(b) Contents of application.—An application under subsection (a) shall include:

(1) The identity and authority of the attorney making the application and the identity of the investigative or law enforcement agency conducting the investigation.

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

(3) An affidavit by an investigative or law enforcement officer which establishes probable cause for the issuance of an order or extension of an order under section 5773.

§ 5773. Issuance of an order for a pen register or a trap and trace device.

(a) In general.—Upon an application made under section 5772 (relating to application for an order for pen registers and trap and trace devices), the court of common pleas shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that there is probable cause to believe that information relevant to an ongoing criminal investigation will be obtained on the telephone line to which the pen register is to be attached.

(b) Contents of order.—An order issued under this section shall:

(1) Specify:

(i) That there is probable cause to believe that information relevant to an ongoing criminal investigation will be obtained on the telephone line to which the pen register or trap and trace device is to be attached.

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

(iii) The identity, if known, of the person who is the subject of the criminal investigation.

(iv) The number and, if known, the physical location of the telephone line to which the pen register or trap and trace device is to be attached, and, in the case of a trap and trace device, the geographical limits of the trap and trace order.

(v) A statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates.

(2) Direct, upon the request of the applicant, the furnishing of information, facilities and technical assistance necessary to accomplish the installation of the pen register under section 5771 (relating to general prohibition of pen register and trap and trace device use; exception).

(c) Time period and extensions.—

(1) An order issued under this section shall authorize the installation and use of a pen register or trap and trace device for a period not to exceed 30 days.

(2) Extensions of such an order may be granted but only upon an application for an order under section 5772 and upon the judicial finding required by subsection (a). The period of each extension shall be for a period not to exceed 30 days.

(d) Nondisclosure of existence of pen register or trap and trace device.—An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that:

(1) The order be sealed until otherwise ordered by the court.

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

§ 5774. Assistance in installation and use of pen registers or trap and trace devices.

(a) Pen registers.—Upon the request of an applicant under this subchapter, a provider of wire or electronic communication service, landlord, custodian or other person shall forthwith provide all information, facilities and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if assistance is directed by a court order as provided in section 5773(b)(2) (relating to issuance of an order for a pen register or a trap and trace device).

(b) Trap and trace device.—Upon the request of an applicant under this subchapter, a provider of a wire or electronic communication service, landlord, custodian or other person shall install the device forthwith on the

appropriate line and shall furnish all additional information, facilities and technical assistance, including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if installation and assistance are directed by a court order as provided in section 5773. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished to the applicant designated in the court at reasonable intervals during regular business hours for the duration of the order.

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

(d) No cause of action against a provider disclosing information under this chapter.—No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents or other specified persons for providing information, facilities or assistance in accordance with the terms of a court order under this subchapter.

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

§ 5775. Reports concerning pen registers.

(a) Attorney General.—The Attorney General shall annually report to the Administrative Office of Pennsylvania Courts on the number of orders for pen registers and trap and trace devices applied for by investigative or law enforcement agencies of the Commonwealth or its political subdivisions.

(b) District attorney.—Each district attorney shall annually provide to the Attorney General information on the number of orders for pen registers and trap and trace devices applied for on forms prescribed by the Attorney General.

SUBCHAPTER F
MISCELLANEOUS

Sec.
5781. Expiration of chapter.

§ 5781. Expiration of chapter.

This chapter expires December 31, 1994, unless extended by statute.

Section 9. The provisions of this act are severable. If any provision of this act or its application to any person or circumstance is held invalid, the invalidity shall not affect other provisions or applications of this act which can be given effect without the invalid provision or application.

Section 10. This act shall take effect immediately.

APPROVED—The 21st day of October, A. D. 1988.

ROBERT P. CASEY