

PENNSYLVANIA CRIMINAL CODE
TITLE 18, CHAPTER 76
COMPUTER OFFENSES

Subchapters

- A. General Provisions
- B. Hacking and Similar Offenses
- C. Internet Child Pornography
- E. Electronic Mail

SUBCHAPTER A
GENERAL PROVISIONS

Sections

- 7601. Definitions.
- 7602. Jurisdiction.
- 7603. Restitution.
- 7604. Concurrent jurisdiction.
- 7605. Defense.
- 7606. Construction.

§ 7601. Definitions.

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

"Access." To intercept, instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system, computer network or database.

"Computer." An electronic, magnetic, optical, hydraulic, organic or other high-speed data processing device or system which performs logic, arithmetic or memory functions and includes all input, output, processing, storage, software or communication facilities which are connected or related to the device in a system or network.

"Computer data." A representation of information, knowledge, facts, concepts or instructions which is being prepared or has been prepared and is intended to be processed, is being processed or has been processed in a computer or computer network and may be in any form, whether readable only by a computer or only by a human or by either, including, but not limited to, computer printouts, magnetic storage media, punched card or stored internally in the memory of the computer.

"Computer network." The interconnection of two or more computers through the usage of satellite, microwave, line or other communication medium.

"Computer operation." Arithmetic, logical, monitoring, storage or retrieval functions and any combination thereof, including, but not limited to, communication with, storage of data to or retrieval of data from any device or human hand manipulation of electronic or magnetic impulses. In reference to a particular computer, the term also includes any function for which that computer was generally designed.

"Computer program." An ordered set of instructions or statements and related data that, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions.

"Computer software." A set of computer programs, procedures or associated documentation concerned with the operation of a computer system.

"Computer system." A set of related, connected or unconnected computer equipment, devices and software.

"Computer virus." A computer program copied to, created on or installed to a computer, computer network, computer program, computer software or computer system without the informed consent of the owner of the computer, computer network, computer program, computer software or computer system that may replicate itself and that causes or can cause unauthorized activities

within or by the computer, computer network, computer program, computer software or computer system.

"Database." A representation of information, knowledge, facts, concepts or instructions which are being prepared or processed or have been prepared or processed in a formalized manner and are intended for use in a computer, computer system or computer network, including, but not limited to, computer printouts, magnetic storage media, punched cards or data stored internally in the memory of the computer.

"Denial-of-service attack." An explicit attempt to prevent legitimate users of a service from using that service, including, but not limited to:

- (1) flooding a network, thereby preventing legitimate network traffic;
- (2) disrupting connections between two computers, thereby preventing access to a service;
- (3) preventing a particular person from accessing a service; or
- (4) disrupting service to a specific computer system or person.

"Deprive." To withhold property of another permanently or for so extended a period as to appropriate a major portion of its economic value, or with intent to restore only upon payment of reward or other compensation, or to dispose of the property so as to make it unlikely that the owner will recover it.

"Economic value." The market value of property or an instrument which creates, releases, discharges or otherwise affects a valuable legal right, privilege or obligation at the time and place of the crime or, if such cannot be satisfactorily ascertained, the cost of replacement of the property or instrument within a reasonable time after the crime.

"Electronic mail service provider." A person who is an intermediary in sending or receiving electronic mail or who provides to end-users of electronic mail services the ability to send or receive electronic mail.

"Electronic mail transmission information." Information used to identify the origin or destination of a transmission or to aid in its routing, including information recorded as part of electronic mail whether or not such information is displayed initially to the user upon receipt of electronic mail, that purports to represent the information used to identify the origin or destination of a transmission or to aid in its routing.

"Established business relationship." A prior or existing relationship formed by a voluntary two-way communication initiated by a person or entity and a recipient with or without an exchange of consideration, on the basis of an inquiry, application purchase or transaction by the recipient regarding products or services offered by such persons or entity. In regard to an inquiry, the person or entity shall obtain the consent of a recipient beyond the initial inquiry. An established business relationship does not exist if the recipient requests to be removed from the distribution lists of an initiator.

"Fax." The transmission of the facsimile of a document through a connection with a telephone or computer network.

"Financial instrument." Includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security or any computer system representation thereof.

"Internet service provider." A person who furnishes a service that enables users to access content, information, electronic mail or other services offered over the Internet.

"Person." Any individual, corporation, partnership, association, organization or entity capable of holding a legal or beneficial interest in property.

"Property." Includes, but is not limited to, financial instruments, computer software and programs in either machine or human readable form, and anything of value, tangible or intangible.

"Telecommunication device." Any type of instrument, device, machine or equipment which is capable of transmitting, acquiring, decrypting or receiving any telephonic, electronic, data, Internet access, audio, video, microwave or radio transmissions, signals, communications or services, including the receipt, acquisition, transmission or decryption of all such communications, transmissions, signals or services over any cable television, telephone, satellite, microwave, radio or wireless distribution system or facility, or any part, accessory or component thereof, including any computer circuit, security module, smart card, software, computer chip, electronic mechanism or other component, accessory or part which is capable of facilitating the transmission, decryption, acquisition or reception of all such communications transmissions, signals or services.

"Wireless advertisement." The initiation of a telephone call or a message capable of providing text, graphic or image messages by a commercial mobile service provider, unlicensed wireless services provider or common carrier wireless exchange access service provider for the purpose of marketing goods or services. The term does not include a call or message to a person with that person's prior express invitation or permission or to a person with whom the caller has an established business relationship.

"World Wide Web." Includes, but is not limited to, a computer server-based file archive accessible over the Internet, using a hypertext transfer protocol, file transfer protocol or other similar protocols.

§ 7602. Jurisdiction.

An offense under this chapter may be deemed to have been committed either at the place where conduct constituting an element of the offense occurred or at the place where the result which is an element of the offense occurred within this Commonwealth in accordance with section 102 (relating to territorial applicability). It shall be no defense to a violation of this chapter that some of the acts constituting the offense occurred outside of this Commonwealth.

§ 7603. Restitution.

Upon conviction of an offense under section 7611 (relating to unlawful use of computer and other computer crimes), 7612 (relating to disruption of service) or 7616 (relating to distribution of computer virus), the sentence shall include an order for restitution to the victim for:

- (1) the cost of repairing or replacing the affected computer, computer system, computer network, computer software, computer program, computer database, World Wide Web site or telecommunication device;
- (2) lost profits for the period that the computer, computer system, computer network, computer software, computer program, computer database, World Wide Web site or telecommunication device is not usable; or
- (3) the cost of replacing or restoring the data lost or damaged as a result of a violation of section 7611, 7612 or 7616.

§ 7604. Concurrent jurisdiction.

The Attorney General shall have concurrent prosecutorial jurisdiction with the county district attorney for violations of this chapter. No person charged with a violation of this section by the Attorney General shall have standing to challenge the authority of the Attorney General to prosecute the case, and, if any such challenge is made, the challenge shall be dismissed and no relief shall be available in the courts of this Commonwealth to the person making the challenge.

§ 7605. Defense.

It is a defense to an action brought pursuant to Subchapter B (relating to hacking and similar offenses) that the actor:

- (1) was entitled by law or contract to engage in the conduct constituting the offense; or
- (2) reasonably believed that he had the authorization or permission of the owner, lessee, licensee, authorized holder, authorized possessor or agent of the computer, computer network, computer software, computer system, database or telecommunication device or that the owner or authorized holder would have authorized or provided permission to engage in the conduct constituting the offense. As used in this section, the term "authorization" includes express or implied consent, including by trade usage, course of dealing, course of performance or commercial programming practices.

§ 7606. Construction.

Nothing in Subchapter B (relating to hacking and similar offenses) shall be construed to interfere with or prohibit terms or conditions in a contract or license related to a computer, computer network, computer software, computer system, database or telecommunication device or software or hardware designed to allow a computer, computer network, computer software, computer system, database or telecommunications device to operate in the ordinary course of a lawful business or that is designed to allow an owner or authorized holder of information to protect data information or rights in it.

SUBCHAPTER B

HACKING AND SIMILAR OFFENSES

Sections

- 7611. Unlawful use of computer and other computer crimes.
- 7612. Disruption of service.
- 7613. Computer theft.
- 7614. Unlawful duplication.
- 7615. Computer trespass.
- 7616. Distribution of computer virus.

§ 7611. Unlawful use of computer and other computer crimes.

- (a) Offense defined.--A person commits the offense of unlawful use of a computer if he:
 - (1) accesses or exceeds authorization to access, alters, damages or destroys any computer, computer system, computer network, computer software, computer program, computer database, World Wide Web site or telecommunication device or any part thereof with the intent to interrupt the normal functioning of a person or to devise or execute any scheme or artifice to defraud or deceive or control property or services by means of false or fraudulent pretenses, representations or promises;
 - (2) intentionally and without authorization accesses or exceeds authorization to access, alters, interferes with the operation of, damages or destroys any computer, computer system, computer network, computer software, computer program, computer database, World Wide Web site or telecommunication device or any part thereof; or
 - (3) intentionally or knowingly and without authorization gives or publishes a password, identifying code, personal identification number or other confidential information about a computer, computer system, computer network, computer database, World Wide Web site or telecommunication device.
- (b) Grading.--An offense under this section shall constitute a felony of the third degree.
- (c) Prosecution not prohibited.--Prosecution for an offense under this section shall not prohibit prosecution under any other section of this title.

§ 7612. Disruption of service.

- (a) Offense defined.--A person commits an offense if he intentionally or knowingly engages in a scheme or artifice, including, but not limited to, a denial of service attack upon any computer, computer system, computer network, computer software, computer program, computer server, computer database, World Wide Web site or telecommunication device or any part thereof that is designed to block, impede or deny the access of information or initiation or completion of any sale or transaction by users of that computer, computer system, computer network, computer software, computer program, computer server or database or any part thereof.
- (b) Grading.--An offense under this section shall constitute a felony of the third degree.

§ 7613. Computer theft.

- (a) Offense defined.--A person commits an offense if he unlawfully accesses or exceeds his authorization to access any data from a computer, computer system or computer network or takes or copies any supporting documentation whether existing or residing internal or external to a computer, computer system or computer network of another with the intent to deprive him thereof.
- (b) Grading.--An offense under this section shall constitute a felony of the third degree.

§ 7614. Unlawful duplication.

- (a) Offense defined.--A person commits the offense of unlawful duplication if he makes or causes to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by or produced by a computer or computer network.
- (b) Grading.--An offense under subsection (a) shall be graded as follows:
 - (1) An offense under this section shall constitute a felony of the third degree.

- (2) If the economic value of the duplicated material is greater than \$2,500, the grading of the offense shall be one grade higher than specified in paragraph (1).

§ 7615. Computer trespass.

- (a) Offense defined.--A person commits the offense of computer trespass if he knowingly and without authority or in excess of given authority uses a computer or computer network with the intent to:
- (1) temporarily or permanently remove computer data, computer programs or computer software from a computer or computer network;
 - (2) cause a computer to malfunction, regardless of the amount of time the malfunction persists;
 - (3) alter or erase any computer data, computer programs or computer software;
 - (4) effect the creation or alteration of a financial instrument or of an electronic transfer of funds; or
 - (5) cause physical injury to the property of another.
- (b) Grading.--An offense under this section shall constitute a felony of the third degree.

§ 7616. Distribution of computer virus.

- (a) Offense defined.--A person commits an offense if the person intentionally or knowingly sells, gives or otherwise distributes or possesses with the intent to sell, give or distribute computer software or a computer program that is designed or has the capability to:
- (1) prevent, impede, control, delay or disrupt the normal operation or use of a computer, computer program, computer software, computer system, computer network, computer database, World Wide Web site or telecommunication device; or
 - (2) degrade, disable, damage or destroy the performance of a computer, computer program, computer software, computer system, computer network, computer database, World Wide Web site or telecommunication device or any combination thereof.
- (b) Grading.--An offense under this section shall constitute a felony of the third degree.

SUBCHAPTER C

INTERNET CHILD PORNOGRAPHY

Sections

- 7621. Definitions.
- 7622. Duty of Internet service provider.
- 7623. Protection of privacy.
- 7624. Penalty.
- 7625. Jurisdiction for prosecution.
- 7626. Application for order to remove or disable items.
- 7627. Order to remove or disable certain items from Internet service provider's service.
- 7628. Notification procedure.
- 7629. Designated agent.
- 7630. Report to General Assembly.

§ 7621. Definitions.

The following words and phrases when used in this subchapter shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Child pornography." As described in section 6312 (relating to sexual abuse of children).

"Internet." The myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected worldwide network of networks that employ the transmission control protocol/Internet protocol or any predecessor or successor protocols to such protocol to communicate information of all kinds by wire or radio.

"Internet service provider." A person who provides a service that enables users to access content, information, electronic mail or other services offered over the Internet.

§ 7622. Duty of Internet service provider.

An Internet service provider shall remove or disable access to child pornography items residing on or accessible through its service in a manner accessible to persons located within this Commonwealth within five business days of when the Internet service provider is notified by the Attorney General pursuant to section 7628 (relating to notification procedure) that child pornography items reside on or are accessible through its service.

§ 7623. Protection of privacy.

Nothing in this subchapter may be construed as imposing a duty on an Internet service provider to actively monitor its service or affirmatively seek evidence of illegal activity on its service.

§ 7624. Penalty.

Notwithstanding any other provision of law to the contrary, any Internet service provider who violates section 7622 (relating to duty of Internet service provider) commits:

- (1) A misdemeanor of the third degree for a first offense punishable by a fine of \$5,000.
- (2) A misdemeanor of the second degree for a second offense punishable by a fine of \$20,000.
- (3) A felony of the third degree for a third or subsequent offense punishable by a fine of \$30,000 and imprisonment for a maximum of seven years.

§ 7625. Jurisdiction for prosecution.

The Attorney General shall have concurrent prosecutorial jurisdiction with the county district attorney for violations of this subchapter. No person charged with a violation of this subchapter by the Attorney General shall have standing to challenge the authority of the Attorney General to prosecute the case. If a challenge is made, the challenge shall be dismissed and no relief shall be available in the courts of this Commonwealth to the person making the challenge.

§ 7626. Application for order to remove or disable items.

An application for an order of authorization to remove or disable items residing on or accessible through an Internet service provider's service shall be made to the court of common pleas having jurisdiction in

writing upon the personal oath or affirmation of the Attorney General or a district attorney of the county wherein the items have been discovered and, if available, shall contain all of the following information:

- (1) A statement of the authority of the applicant to make the application.
- (2) A statement of the identity of the investigative or law enforcement officer that has, in the official scope of that officer's duties, discovered the child pornography items.
- (3) A statement by the investigative or law enforcement officer who has knowledge of relevant information justifying the application.
- (4) The Uniform Resource Locator providing access to the items.
- (5) The identity of the Internet service provider used by the law enforcement officer.
- (6) A showing that there is probable cause to believe that the items constitute a violation of section 6312 (relating to sexual abuse of children).
- (7) A proposed order of authorization for consideration by the judge.
- (8) Contact information for the Office of Attorney General, including the name, address and telephone number of any deputy or agent authorized by the Attorney General to submit notification.
- (9) Additional testimony or documentary evidence in support of the application as the judge may require.

§ 7627. Order to remove or disable certain items from Internet service provider's service.

Upon consideration of an application, the court may enter an order, including an ex parte order as requested, advising the Attorney General or a district attorney that the items constitute probable cause evidence of a violation of section 6312 (relating to sexual abuse of children) and that such items shall be removed or disabled from the Internet service provider's service. The court may include such other information in the order as the court deems relevant and necessary.

§ 7628. Notification procedure.

- (a) Duty of Attorney General.--The Attorney General shall have exclusive jurisdiction to notify Internet service providers under this subchapter. The Attorney General shall initiate notification under this subchapter if requested in writing by a district attorney who has provided the Attorney General with a copy of an application made under section 7626 (relating to application to remove or disable items) and a copy of the order issued under section 7627 (relating to order to remove or disable certain items from Internet service provider's service) or upon the issuance of an order based upon an application filed by the Attorney General.
- (b) Timely notification.--For purposes of this section, an Internet service provider or the person designated by the Internet service provider as provided for in section 7629 (relating to designated agent) shall be notified in writing by the Attorney General within three business days of the Attorney General's receipt of an order.
- (c) Contents.--The notice shall include the following information:
 - (1) A copy of the application made under section 7626.
 - (2) A copy of the court order issued under section 7627.
 - (3) Notification that the Internet service provider must remove or disable the items residing on or accessible through its service within five business days of the date of receipt of the notification.
 - (4) Contact information for the Office of Attorney General, including the name, address and telephone number of any deputy or agent authorized by the Attorney General to submit notification pursuant to this subsection.

§ 7629. Designated agent.

An Internet service provider may designate an agent to receive notification provided under section 7628 (relating to notification procedure).

§ 7630. Report to General Assembly.

The Attorney General shall make an annual report to the chairman and minority chairman of the Judiciary Committee of the Senate and to the chairman and minority chairman of the Judiciary Committee of the House of Representatives providing information on the number of notifications issued and the prosecutions made under this subchapter and making any recommendations for amendatory language.

SUBCHAPTER E ELECTRONIC MAIL

Sections

7661. Unlawful transmission of electronic mail.

§ 7661. Unlawful transmission of electronic mail.

- (a) Offense defined.--A person commits the offense of unlawful transmission of electronic mail if he:
- (1) Uses a computer or computer network without authority and with the intent to falsify or forge electronic mail transmission information or other routine information in any manner in connection with the transmission of unsolicited electronic mail through or into the computer network of an electronic mail service provider, Internet service provider or its subscribers.
 - (2) Sells, gives or otherwise distributes or possesses with the intent to sell, give or distribute computer software which:
 - (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information;
 - (ii) has only limited commercially significant purpose or use other than to facilitate or to enable the falsification of electronic mail transmission information or other routing information; or
 - (iii) is marketed by that person or another person acting in concert with that person with that person's knowledge for the use in facilitating or enabling the falsification of electronic mail transmission information or other routing information.
- (b) Grading.--
- (1) Except as provided in paragraphs (2) and (3), unlawful transmission of electronic mail is a misdemeanor of the third degree punishable by a fine of not more than \$2,500.
 - (2) If there is damage to the property of another valued at \$2,500 or more caused by that person's reckless disregard for the consequences of his act in violation of this section, unlawful transmission of electronic mail is a misdemeanor of the first degree punishable by a fine of not more than \$10,000.
 - (3) If there is damage to the property of another valued at \$2,500 or more caused by that person's malicious act in violation of this section, unlawful transmission of electronic mail is a felony of the third degree punishable by a fine of not more than \$15,000.
- (c) Rights preserved.--Nothing in this section shall be construed to:
- (1) Establish any liability by reason of terms or conditions adopted by or technical measures implemented by an electronic mail service provider or Internet service provider doing business in this Commonwealth to prevent the transmission of unsolicited electronic mail in violation of this section.
 - (2) Interfere with or prohibit terms or conditions in a contract or license related to computers, computer data, computer networks, computer operations, computer programs, computer services or computer software.
- (d) Definitions.--As used in this section, the term "*electronic mail*" shall include facsimiles and wireless advertisements in addition to other electronic mail.