Stricken language would be deleted from and underlined language would be added to the law as it existed prior to this session of the General Assembly.

State of Arkansas
83rd General Assembly
Regular Session, 2001

A Bill

SENATE BILL 953

By: Senator B. Walker

For An Act To Be Entitled

AN ACT TO ADDRESS COMPUTER CRIMES; AND FOR OTHER PURPOSES.

Subtitle

AN ACT TO ADDRESS COMPUTER CRIMES.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF ARKANSAS:

SECTION 1. Arkansas Code Title 5, Chapter 27 is amended by adding an additional subchapter to read as follows:

Subchapter 6 -- Computer Crimes Against Minors

5-27-601. Definitions.

For purposes of this subchapter:

(1) "Child" means any person under seventeen (17) years of age;

(2)(A) "Computer" means an electronic, magnetic, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with the device.

(B) "Computer" also includes any on-line service, internet service, or local bulletin board, any electronic storage device, including a floppy disk or other magnetic storage device, or any compact disk that has read-only memory and the capacity to store audio, video, or written materials;

(3) "Computer network" means the interconnection of communications lines with a computer through remote terminals or a complex consisting of two (2) or more interconnected computers;

(4) "Computer program" means a set of instructions, statements, or

related data that, in actual or modified form, is capable of causing a computer or a computer system to perform specified functions;

(5) "Computer software" means one (1) or more computer programs, existing in any form, or any associated operational procedures, manuals, or other documentation;

(6) "Computer system" means a set of related, connected, or unconnected computers, other devices, and software;

(7) "Internet" means the international computer network of both federal and non-federal interoperable packet switched data networks;

(8) "Performance" means any play, dance, act, drama, piece, interlude, pantomime, show, scene, or other three-dimensional presentation or parts whether performed live or photographed, filmed, videotaped, or visually depicted by any other photographic, cinematic, magnetic, or electronic means;

(9) "Reproduction" means, but is not limited to, computer-generated images;

(10) "Sexual intercourse" means penetration, however slight, of the labia majora by a penis; and

(11) "Sexually explicit conduct" means actual or simulated:

(A) Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

(B) Bestiality;

(C) Masturbation;

(D) Sadomasochistic abuse for the purpose of sexual stimulation; or

(E) Lewd exhibition of:

(i) The genitals or pubic area of any person; or

(ii) The breast of a female.

5-27-602. Distributing, possessing, or viewing matter depicting sexually explicit conduct involving a child.

(a) A person commits distributing, possessing, or viewing of matter depicting sexually explicit conduct involving a child if the person knowingly receives for the purpose of selling or knowingly sells, procures, manufactures, gives, provides, lends, trades, mails, delivers, transfers, publishes, distributes, circulates, disseminates, presents, exhibits,

advertises, offers, or agrees to offer, through any means, including the internet, any photograph, film, videotape, computer program, or file, computer-generated image, video game, or any other reproduction or reconstruction which depicts a child engaging in sexually explicit conduct.

(b) Distributing, possessing, or viewing of matter depicting sexually explicit conduct involving a child is a:

(1) Class C felony for the first offense; and

(2) Class B felony for any subsequent offenses.

5-27-603. Computer child pornography.

(a)(1) A person commits computer child pornography in the first degree if the person:

(A) Knowingly compiles, enters into, or transmits by means of computer, makes, prints, publishes, or reproduces by other computerized means, knowingly causes or allows to be entered into or transmitted by means of computer, or buys, sells, receives, exchanges, or disseminates, any notice, statement, or advertisement, or any child's name, telephone number, place of residence, physical characteristics, or other descriptive or identifying information, for purposes of facilitating, encouraging, offering, or soliciting sexually explicit conduct of or with any child or another individual believed by the person to be a child, or the visual depiction of the conduct; or

(B) Knowingly utilizes a computer online service, internet service, or local bulletin board service to seduce, solicit, lure, or entice, or attempt to seduce, solicit, lure, or entice, a child or another individual believed by the person to be a child, to engage in sexually explicit conduct.

(2) Computer child pornography in the first degree is a Class B felony.

(b)(1) A person commits computer child pornography in the second degree if the person:

(A) Is the owner or operator of a computer online service, internet service, or local bulletin board service; and

(B) The person knowingly permits a subscriber to utilize the service to commit a violation of this subchapter.

(2) Computer pornography in the second degree is a Class A misdemeanor.

5-27-604. Computer exploitation of a child.

(a)(1) A person commits computer exploitation of a child in the first degree if the person causes or permits a child to engage in sexually explicit conduct if the person knows, has reason to know, or intends that the prohibited conduct may be photographed, filmed, reproduced, or reconstructed in any manner, including on the internet, or may be part of an exhibition or performance.

(2)(A) Computer exploitation of a child in the first degree is a Class C felony for the first offense.

(B) Computer exploitation of a child in the first degree is a Class B felony for the second and subsequent offenses.

(3) Computer exploitation of a child in the first degree shall be a Class B felony if the person is the parent, guardian, or other person legally charged with the care or custody of the child.

(b)(1) A person commits computer exploitation of a child in the second degree if the person photographs or films a child engaged in sexually explicit conduct or uses any device, including a computer, to reproduce or reconstruct the image of a child engaged in sexually explicit conduct.

(2) Exploitation of a child in the second degree is a Class D felony.

5-27-605. Jurisdiction.

For the purpose of determining jurisdiction, a person is subject to prosecution in this state for any conduct proscribed by this subchapter, if the transmission that constitutes the offense either originates in this state or is received in this state.

5-27-606. Determination of age of child.

(a) For purposes of this subchapter, the state must prove beyond a reasonable doubt that the child who is depicted as or presents the appearance of being under the age of seventeen (17) in any photograph, film, videotape, computer program or file, computer-generated image, video game, or any other reproduction or reconstruction is under the age of seventeen (17).

(b) If it becomes necessary for purposes of this subchapter to determine whether a child depicted engaging in sexually explicit conduct, was

under seventeen (17) years of age, the court or jury may make this determination by any of the following methods:

(1) Personal inspection of the child;

(2) Inspection of the photograph, film, videotape, computer program or file, computer-generated image, video game, or any other reproduction or reconstruction picture that depicts the child engaging in the sexually explicit conduct;

(3) Expert medical testimony based on the appearance of the child engaged in the sexually explicit conduct; or

(4) Any other method authorized by law.

SECTION 2. Arkansas Code Title 5, Chapter 41 is amended by adding an additional subchapter to read as follows:

Subchapter 2-- Unlawful Computer Crimes

5-41-201. Definitions.

For purposes of this subchapter:

(1) "Access" means to intercept, instruct, communicate with, store data in, retrieve from or otherwise make use of any resources of a computer, network, or data;

(2)(A) "Computer" means an electronic, magnetic, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with the device.

(B) "Computer" also includes any on-line service, internet service, or local bulletin board, any electronic storage device, including a floppy disk or other magnetic storage device, or any compact disk that has read-only memory and the capacity to store audio, video, or written materials;

(3)(A) "Computer contaminant" means any data, information, image, program, signal, or sound that is designed or has the capability to:

(i) Contaminate, corrupt, consume, damage, destroy, disrupt, modify, record, or transmit; or

(ii) Cause to be contaminated, corrupted, consumed, damaged, destroyed, disrupted, modified, recorded, or transmitted, any other data, information, image, program, signal, or sound contained in a computer, system or network without the knowledge or consent of the person who owns the

other data, information, image, program, signal or sound, or the computer, system or network.

(B) "Computer contaminant" includes but is not limited to:

(i) A virus, worm, or Trojan horse; or

(ii) Any other similar data, information, image, program, signal or sound that is designed or has the capability to prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system, or network;

(4) "Data" means a representation of any form of information, knowledge, facts, concepts, or instructions which is being prepared or has been formally prepared and is intended to be processed, is being processed, or has been processed in a system or network;

(5) "Encryption" means the use of any protection or disruptive measure, including, without limitation, cryptography, enciphering, encoding, or a computer contaminant, to:

(A) Prevent, impede, delay or disrupt access to any data, information, image, program, signal, or sound;

(B) Cause or make any data, information, image, program, signal, or sound unintelligible or unusable; or

(C) Prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system, or network;

(6) "Information service" means a service that is designed or has the capability to generate, process, store, retrieve, convey, emit, transmit, receive, relay, record, or reproduce any data, information, image, program, signal, or sound by means of any component, device, equipment, system, or network, including, but not limited to, by means of:

(A) A computer, computer system, computer network, modem, or scanner;

(B) A telephone, cellular phone, satellite phone, pager, personal communications device, or facsimile machine;

(C) Any type of transmitter or receiver; or

(D) Any other component, device, equipment, system, or network that uses analog, digital, electronic, electromagnetic, magnetic, or optical technology;

(7)(A) "Network" means a set of related, remotely connected devices and facilities, including more than one (1) system, with the capability to

transmit data among any of the devices and facilities.

(B) "Network" includes, but is not limited to, a local, regional, or global computer network;

(8) "Program" means an ordered set of data representing coded instructions, or statements which can be executed by a computer and cause the computer to perform one or more tasks;

(9) "Property" means anything of value and includes a financial instrument, information, electronically produced data, program, and any other tangible or intangible item of value.

(10) "Provider" means any person who provides an information service;

(11) "Provider of internet service" means any provider who provides subscribers with access to the internet or an electronic mail address or both; and

(12) "System" means a set of related equipment, whether or not connected, which is used with or for a computer.

5-41-202. Unlawful acts regarding computers.

(a) A person commits an unlawful act regarding a computer if the person knowingly and without authorization:

(1) Modifies, damages, destroys, discloses, uses, transfers, conceals, takes, retains possession of, copies, obtains or attempts to obtain access to, permits access to or causes to be accessed, or enters data or a program which exists inside or outside a computer, system, or network;

(2) Modifies, destroys, uses, takes, damages, transfers, conceals, copies, retains possession of, obtains or attempts to obtain access to, permits access to or causes to be accessed, equipment or supplies that are used or intended to be used in a computer, system, or network;

(3) Destroys, damages, takes, alters, transfers, discloses, conceals, copies, uses, retains possession of, obtains or attempts to obtain access to, permits access to or causes to be accessed, a computer, system, or network;

(4) Obtains and discloses, publishes, transfers, or uses a device used to access a computer, network, or data; or

(5) Introduces, causes to be introduced or attempts to introduce a computer contaminant into a computer, system, or network.

(b) An unlawful act regarding a computer is a Class A misdemeanor.

(c) An unlawful act regarding a computer shall be a Class C felony if the act:

(1) Was committed to devise or execute a scheme to defraud or illegally obtain property;

(2) Caused damage in excess of five hundred dollars ($500); or

(3) Caused an interruption or impairment of a public service, including, without limitation, a governmental operation, a system of public communication or transportation, or a supply of water, gas, or electricity.

5-41-203. Unlawful interference with access to computers - Unlawful use or access of computers.

(a)(1) A person commits unlawful interference with access to computers if the person knowingly and without authorization interferes with, denies, or causes the denial of access to or use of a computer, system, or network to a person who has the duty and right to use it.

(2) Unlawful interference with access to computers is a Class A misdemeanor.

(b)(1) A person commits unlawful use or access to computers if the person knowingly and without authorization uses, causes the use of, accesses, attempts to gain access to, or causes access to be gained to a computer, system, network, telecommunications device, telecommunications service, or information service.

(2) Unlawful use or access to computers is a Class A misdemeanor.

(c) If the violation of subsections (a) or (b) of this section was committed to devise or execute a scheme to defraud or illegally obtain property, the person is guilty of a Class C felony;

(d) It is an affirmative defense to a charge made pursuant to this section that at the time of the alleged offense the person reasonably believed that:

(1) The person was authorized to use or access the computer, system, network, telecommunications device, telecommunications service, or information service and the use or access by the person was within the scope of that authorization; or

(2) The owner or other person authorized to give consent would authorize the person to use or access the computer, system, network,

telecommunications device, telecommunications service, or information service.

(e) A person who intends to offer an affirmative defense provided in subsection (d) of this section at a trial or preliminary hearing shall, not less than fourteen (14) calendar days before the trial or hearing or at such other time as the court may direct, file and serve on the prosecuting attorney a notice of that intent.

5-41-204. Unlawful use of encryption.

(a) A person commits unlawful use of encryption if the person knowingly uses or attempts to use encryption, directly or indirectly, to:

(1) Commit, facilitate, further, or promote any criminal offense;

(2) Aid, assist, or encourage another person to commit any criminal offense;

(3) Conceal the commission of any criminal offense;

(4) Conceal or protect the identity of a person who has committed any criminal offense; or

(5) Delay, hinder, or obstruct the administration of the law.

(b) A person who violates any provision of this section commits a criminal offense that is separate and distinct from any other criminal offense and may be prosecuted and convicted pursuant to this section whether or not the person or any other person is or has been prosecuted or convicted for any other criminal offense arising out of the same facts as the violation of this section.

(c)(1) Unlawful use of encryption is a Class D felony if the criminal offense concealed by encryption is a Class Y, Class A, or Class B felony.

(2) Unlawful use of encryption is a Class A misdemeanor if the criminal offense concealed by encryption is a Class C or Class D felony, or an unclassified felony.

(3) Other unlawful uses of encryption shall be a misdemeanor classed one (1) degree below the misdemeanor constituted by the criminal offense concealed by encryption.

5-41-205. Unlawful acts involving electronic mail.

(a) A person commits an unlawful act involving electronic mail if the

person:

(1) Knowingly:

(A) Falsifies or forges any data, information, image, program, signal, or sound that is contained in the header, subject line, or routing instructions of an item of electronic mail; or

(B) Describes or identifies the sender, source, point of origin or path of transmission of an item of electronic mail, with the purpose to transmit or cause to be transmitted the item of electronic mail to the electronic mail address of one or more recipients without their knowledge of or consent to the transmission;

(2) Purposely transmits or causes to be transmitted an item of electronic mail to the electronic mail address of one or more recipients without their knowledge of or consent to the transmission, if the person knows or has reason to know that the item of electronic mail contains or has been generated or formatted with:

(A) An internet domain name that is being used without the consent of the person who holds the internet domain name; or

(B) Any data, information, image, program, signal, or sound that has been used intentionally in the header, subject line or routing instructions of the item of electronic mail to falsify or misrepresent:

(i) The identity of the sender; or

(ii) The source, point of origin or path of transmission of the item of electronic mail; or

(3) Knowingly sells, gives, or otherwise distributes or possesses with the intent to sell, give, or otherwise distribute any data, information, image, program, signal, or sound which is designed or intended to be used to falsify or forge any data, information, image, program, signal, or sound that:

(A) Is contained in the header, subject line, or routing instructions of an item of electronic mail; or

(B) Describes or identifies the sender, source, point of origin, or path of transmission of an item of electronic mail.

(b) Subdivision (a)(2) does not apply to a provider of internet service who, in the course of providing service, transmits, or causes to be transmitted an item of electronic mail on behalf of another person, unless the provider of internet service is the person who first generates the item

of electronic mail.

(c) An unlawful act involving electronic mail is a Class A misdemeanor.

(d) If the violation of subsection (a) of this section was committed to devise or execute a scheme to defraud or illegally obtain property, the person is guilty of a Class C felony.

5-41-206. Computer password disclosure.

(a) A person commits computer password disclosure if the person purposely and without authorization discloses a number, code, password, or other means of access to a computer or computer network.

(b) Computer password disclosure is a Class A misdemeanor.

(c) If the violation of subsection (a) of this section was committed to devise or execute a scheme to defraud or illegally obtain property, the person is guilty of a Class D felony.

SECTION 3. Arkansas Code § 12-12-903(13)(A) is amended to read as follows:

(13) "Sex offense" means:

(A)(i) Rape, § 5-14-103;

(ii) Carnal abuse in the first degree, § 5-14-104;

(iii) Carnal abuse in the second degree, § 5-14-105;

(iv) Carnal abuse in the third degree, § 5-14-106;

(v) Sexual misconduct, § 5-14-107;

(vi) Sexual abuse in the first degree, § 5-14-108;

(vii) Sexual abuse in the second degree, § 5-14-109;

(viii) Sexual solicitation of a child, § 5-14-110;

(ix) Violation of a minor in the first degree, § 5-14-120;

(x) Violation of a minor in the second degree, § 5-14-121;

(xi) Incest, § 5-26-202;

(xii) Engaging children in sexually explicit conduct for use in visual or print medium, § 5-27-303;

(xiii) Transportation of minors for prohibited sexual conduct, § 5-27-305;

(xiv) Employing or consenting to use of child in sexual performance, § 5-27-402;

(xv) Producing, directing, or promoting sexual performance, § 5-27-403;

(xvi) Promoting prostitution in the first degree, § 5-70-104;

(xvii) Stalking, § 5-71-229;

(xviii) Indecent exposure to a person under the age of twelve (12) years, § 5-14-112(b); ~~or~~

(xix) Exposing another person to human immunodeficiency virus, § 5-14-123;

(xx) Computer child pornography in the first degree; or

(xxi) Computer exploitation of a child in the first degree;