Senate Bill 103

By: Senator Lamutt of the 21st

A BILL TO BE ENTITLED

AN ACT

To amend Article 6 of Chapter 9 of Title 16 of the Official Code of Georgia Annotated, relating to computer systems protection, so as to create the offense of computer trespass in the second degree; to enact the "Internet and Computer Safety Act"; to provide definitions; to provide for the offense of obscene Internet contact with a child; to provide for the offense of harassing e-mails; to provide penalties; to provide that the Attorney General may have concurrent jurisdiction with county district attorneys under this article; to provide for investigative authority and criminal procedures; to provide for disclosure requirements in criminal investigations; to provide for forfeiture proceedings; to amend Article 2 of Chapter 5 of Title 17 of the Official Code of Georgia Annotated, relating to searches with warrants, so as to provide for procedures for search warrants issued to certain electronic communication services or remote computing services; to amend Code Section 16-11-37, relating to terroristic threats, so as to make it unlawful to use a computer or other electronic means to make terroristic threats; to amend Article 3 of Chapter 12 of Title 16 of the Official Code of Georgia Annotated, relating to obscenity and related offenses, so as to change certain penalty provisions applicable to offenses relating to minors; to require Internet service providers to remove or disable access to child pornography items under certain conditions; to provide for other matters relative thereto; to provide for an effective date; to repeal conflicting laws; and for other purposes.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

SECTION 1.

Code Sections 16-9-90 through 16-9-94 are designated as Part 1 of Article 6 of Chapter 9.

SECTION 2.

Article 6 of Chapter 9 of Title 16 of the Official Code of Georgia Annotated, known as the "Georgia Computer Systems Protection Act," is amended by striking in their entirety Code Sections 16-9-90, 16-9-92, 16-9-93, and 16-9-94 and inserting in lieu thereof the following:

"16-9-90.

This ~~article~~ part shall be known and may be cited as the 'Georgia Computer Systems Protection Act.'"

"16-9-92.

As used in this ~~article~~ part, the term:

(1) 'Computer' means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device or system performing computer operations with or on data and includes any data storage facility or communications facility directly related to or operating in conjunction with such device; but such term does not include an automated typewriter or typesetter, portable hand-held calculator, household appliance, or other similar device that is not used to communicate with or to manipulate any other computer.

(2) 'Computer network' means a set of related, remotely connected computers and any communications facilities with the function and purpose of transmitting data among them through the communications facilities.

(3) 'Computer operation' means computing, classifying, transmitting, receiving, retrieving, originating, switching, storing, displaying, manifesting, measuring, detecting, recording, reproducing, handling, or utilizing any form of data for business, scientific, control, or other purposes.

(4) 'Computer program' means one or more statements or instructions composed and structured in a form acceptable to a computer that, when executed by a computer in actual or modified form, cause the computer to perform one or more computer operations. The term 'computer program' shall include all associated procedures and documentation, whether or not such procedures and documentation are in human readable form.

(5) 'Data' includes any representation of information, intelligence, or data in any fixed medium, including documentation, computer printouts, magnetic storage media, punched cards, storage in a computer, or transmission by a computer network.

(6) 'Financial instruments' includes any check, draft, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction-authorizing mechanism, or marketable security, or any computer representation thereof.

(7) 'Property' includes computers, computer networks, computer programs, data, financial instruments, and services.

(8) 'Services' includes computer time or services or data processing services.

(9) 'Use' includes causing or attempting to cause:

(A) A computer or computer network to perform or to stop performing computer operations;

(B) The obstruction, interruption, malfunction, or denial of the use of a computer, computer network, computer program, or data; or

(C) A person to put false information into a computer.

(10) 'Victim expenditure' means any expenditure reasonably and necessarily incurred by the owner to verify that a computer, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by unauthorized use.

(11) 'Without authority' includes the use of a computer or computer network in a manner that exceeds any right or permission granted by the owner of the computer or computer network.

16-9-93.

(a) *Computer Theft.* Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

(1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession;

(2) Obtaining property by any deceitful means or artful practice; or

(3) Converting property to such person´s use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property

shall be guilty of the crime of computer theft.

(b) *Computer Trespass.*

(1) Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

~~(1)~~(A) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;

~~(2)~~(B) Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or

~~(3)~~(C) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists

shall be guilty of the crime of computer trespass.

(2) Any person who uses a computer or computer network with knowledge that such use is without authority shall be guilty of the crime of computer trespass in the second degree.

(c) *Computer Invasion of Privacy.* Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy.

(d) *Computer Forgery.* Any person who creates, alters, or deletes any data contained in any computer or computer network, who, if such person had created, altered, or deleted a tangible document or instrument would have committed forgery under Article 1 of this chapter, shall be guilty of the crime of computer forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to the crime of computer forgery if a creation, alteration, or deletion of data was involved in lieu of a tangible document or instrument.

(e) *Computer Password Disclosure.* Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of $500.00 shall be guilty of the crime of computer password disclosure.

(f) ~~*Article*~~ *Part not Exclusive.* The provisions of this ~~article~~ part shall not be construed to preclude the applicability of any other law which presently applies or may in the future apply to any transaction or course of conduct which violates this ~~article~~ part.

(g) *Civil Relief; Damages.*

(1) Any person whose property or person is injured by reason of a violation of any provision of this ~~article~~ part may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, 'damages' shall include loss of profits and victim expenditure.

(2) At the request of any party to an action brought pursuant to this Code section, the court shall by reasonable means conduct all legal proceedings in such a way as to protect the secrecy and security of any computer, computer network, data, or computer program involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party.

(3) The provisions of this ~~article~~ part shall not be construed to limit any person´s right to pursue any additional civil remedy otherwise allowed by law.

(4) A civil action under this Code section must be brought within four years after the violation is discovered or by exercise of reasonable diligence should have been discovered. For purposes of this ~~article~~ part, a continuing violation of any one subsection of this Code section by any person constitutes a single violation by such person.

(h) *Criminal Penalties.*

(1) Any person convicted of the crime of computer theft, computer trespass, computer invasion of privacy, or computer forgery shall be fined not more than $50,000.00 or imprisoned not more than 15 years, or both.

(2) Any person convicted of computer password disclosure shall be fined not more than $5,000.00 or incarcerated for a period not to exceed one year, or both.

(3) Any person convicted of the crime of computer trespass in the second degree shall be punished as for a misdemeanor.″

″16-9-94.

For the purpose of venue under this ~~article~~ part, any violation of this ~~article~~ part shall be considered to have been committed:

(1) In the county of the principal place of business in this state of the owner of a computer, computer network, or any part thereof;

(2) In any county in which any person alleged to have violated any provision of this ~~article~~ part had control or possession of any proceeds of the violation or of any books, records, documents, or property which were used in furtherance of the violation;

(3) In any county in which any act was performed in furtherance of any transaction which violated this ~~article~~ part; and

(4) In any county from which, to which, or through which any use of a computer or computer network was made, whether by wires, electromagnetic waves, microwaves, or any other means of communication.″

SECTION 3.

Said article is further amended by inserting after Code Section 16-9-94 a new Part 2, which part shall be known as and may be cited as the "Internet and Computer Safety Act," which shall consist of new Code Sections 16-9-100, 16-9-101, 16-9-102, 16-9-103, 16-9-104, and 16-9-105 to read as follows:

″Part 2

16-9-100.

As used in this part, the term:

(1) 'Electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic, or photo optical system that affects interstate or foreign commerce, but does not include:

(A) Any wire or oral communication;

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

(C) Any communication from a tracking device; or

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

(2) 'Electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications.

(3) 'Electronic communications system' means any wire, radio, electromagnetic, photo optical, or photo electronic facilities for the transmission of wire or electronic communications and any computer facilities or related electronic equipment for the electronic storage of such communications.

(4) 'Electronic means' is any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than:

(A) Any telephone or telegraph instrument, equipment, or facility, or any component thereof that is:

(i) Furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or

(ii) Being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his or her duties; or

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

(5) 'Electronic storage' means:

(A) Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) Any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

(6) 'Law enforcement agency' means:

(A) Any agency, organ, or department of this state, a subdivision or municipality thereof, or a railroad whose primary functions include the enforcement of criminal or traffic laws, the preservation of public order, the protection of life and property, or the prevention, detection, or investigation of crime;

(B) The Office of Permits and Enforcement of the Department of Transportation, the Department of Juvenile Justice and its institutions and facilities for the purpose of personnel who are authorized to exercise the power of arrest and who are employed or appointed by said department or institutions, and the office or section in the Department of Juvenile Justice in which persons are assigned who have been designated by the commissioner of juvenile justice to investigate and apprehend unruly and delinquent children; and

(C) The Department of Corrections, the State Board of Pardons and Paroles, municipal correctional institutions employing 300 or more correctional officers, and county correctional institutions for the purpose of personnel who are authorized to exercise the power of arrest and who are employed or appointed by said department, board, or institutions.

(7) 'Remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.

(8) 'Solicitor general' means any solicitor employed on a full-time basis as determined by the General Assembly under the provisions of Code Section 15-18-63 and who is not engaged in the private practice of law.

(9) 'Telemarketing' means:

(A) A plan, program, promotion, or campaign that is conducted to induce:

(i) Purchases of goods or services;

(ii) Participation in a contest or sweepstakes; or

(iii) A charitable contribution, donation, or gift of money or any other thing of value by use of one or more interstate telephone calls initiated either by a person who is conducting the plan, program, promotion, or campaign or by a prospective purchaser, contest or sweepstakes participant, or charitable contributor or donor; but

(B) Does not include the solicitation of sales through the mailing of a catalog that:

(i) Contains a written description or illustration of the goods or services offered for sale;

(ii) Includes the business address of the seller;

(iii) Includes multiple pages of written material or illustration; and

(iv) Has been issued not less frequently than once a year if the person making the solicitation does not solicit customers by telephone but only receives calls initiated by customers in response to the catalog and during those calls takes orders without further solicitation.

(10) 'Tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object.

16-9-101.

(a) A person commits the offense of obscene Internet contact with a child if that person has contact with any person under the age of 18 years that is not his or her spouse via electronic means, including, but not limited to, e-mail or an Internet chatroom, who that person believes is a child under the age of 18 years and that contact involves any matter containing explicit verbal descriptions or narrative accounts of sexually explicit nudity, sexual conduct, sexual excitement, or sadomasochistic abuse which is intended to arouse

or satisfy the sexual desire of either the child or the person, provided that no conviction shall be had for this offense on the unsupported testimony of the victim.

(b) A person commits the offense of harassing e-mails if:

(1) Such person e-mails another person repeatedly for the purpose of annoying or harassing another person or the family of such other person;

(2) Via e-mail, uses language threatening bodily harm; or

(3) Knowingly permits an e-mail account under such person´s control to be used for any purpose prohibited by this subsection.

(c) A person convicted of the offense of obscene Internet contact with a child shall be guilty of a felony and punished by imprisonment for not less than one nor more than ten years; provided, however, that if the victim is between the ages of 14 and 18 and the person so convicted is no more than four years older than the victim, such person shall be guilty of a misdemeanor.

(d) Any person who commits the offense of harassing e-mails shall be guilty of a misdemeanor.

(e) The sole fact that an undercover operative or law enforcement officer was involved in the detection and investigation of an offense under this Code section shall not constitute a defense to prosecution under this Code section.

16-9-102.

The Attorney General, at his or her discretion, and the district attorneys shall have concurrent authority to conduct criminal prosecutions and bring other actions under this article.

16-9-103.

(a) In any investigation of a violation of this article or any other criminal offense involving the use of a computer in furtherance of the crime, the Attorney General, any district attorney, or any solicitor-general shall have the power to administer oaths; to call any party to testify under oath at such investigations; to require the attendance of witnesses and the production of books, records, and papers; and to take the depositions of witnesses. The Attorney General, any district attorney, or any solicitor-general is authorized to issue a subpoena for any witness or a subpoena to compel the production of any books, records, or papers.

(b) In a case of refusal to obey a subpoena issued under this Code section to any person and upon application by the Attorney General, district attorney, or solicitor-general, the superior court in whose jurisdiction the witness is to appear or in which the books, records, or papers are to be produced may issue to that person an order requiring him or her to

appear before the court to show cause why he or she should not be held in contempt for refusal to obey the subpoena. Failure to obey a subpoena may be punished by the court as contempt of court.

16-9-104.

(a) Any law enforcement agency, the Attorney General, district attorney, or solicitor-general who is conducting an investigation of a violation of this article or other criminal offense involving the use of a computer in furtherance of the crime may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication that is in electronic storage in an electronic communications system for 180 days or less pursuant to a search warrant issued under the provisions of Article 2 of Chapter 5 of Title 17, relating to searches with warrants by a court with jurisdiction over the offense under investigation. Said court may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than 180 days by the means available under subsection (c) of this Code section.

(b)(1) Any law enforcement agency, the Attorney General, district attorney, or solicitor-general may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection:

(A) Without required notice to the subscriber or customer if an officer obtains a search warrant pursuant to Article 2 of Chapter 5 of Title 17; or

(B) With prior notice from the law enforcement agency, the Attorney General, district attorney, or solicitor-general to the subscriber or customer if the law enforcement agency, the Attorney General, district attorney, or solicitor-general:

(i) Uses an administrative subpoena authorized by Code Sections 16-9-103 or 45-15-17, a grand jury subpoena, or a trial subpoena; or

(ii) Obtains a court order for such disclosure under subsection (d) of this Code section, except that notice to the subscriber or customer may be delayed as provided in paragraph (e) of this Code section.

(2) The provisions of paragraph (1) of this subsection are applicable with respect to any wire or electronic communication that is held or maintained on that service:

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

(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer if the provider is not authorized to access the contents of any

such communications for purposes of providing any services other than storage or computer processing.

(c)(1) Any law enforcement agency, the Attorney General, district attorney, or solicitor-general may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service, not including the contents of communications, only when any law enforcement agency, the Attorney General, district attorney, or solicitor-general:

(A) Obtains a search warrant as provided in Article 2 of Chapter 5 of Title 17;

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

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

(D) Submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing, as such term is defined in 16-9-100; or

(E) Seeks information under paragraph (2) of this subsection.

(2) A provider of electronic communication service or remote computing service shall disclose to any law enforcement agency, the Attorney General, district attorney, or solicitor-general the following information:

(A) Name;

(B) Address;

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

(D) Length of service, start date of service, and types of service utilized;

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

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

of a subscriber to or customer of such service when any law enforcement agency, the Attorney General, district attorney, or solicitor-general uses an administrative subpoena authorized by Code Section 16-9-103 or 45-15-17, a grand jury or trial subpoena, or any means available under paragraph (1) of this subsection.

(3) Any law enforcement agency, the Attorney General, district attorney, or solicitor-general receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) A court order for disclosure under subsection (b) or (c) of this Code section may be issued by any court that is a superior court with jurisdiction over the offense under investigation and shall be issued only if a law enforcement agency, the Attorney General,

district attorney, or solicitor-general offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. A court issuing an order pursuant to this Code section may quash or modify such order on a motion made promptly by the service provider if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e)(1) Any law enforcement agency, the Attorney General, district attorney, or solicitor-general who is acting under this Code section may:

(A) Where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under this Code section for a period not to exceed 90 days if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) Where an administrative subpoena, a state grand jury subpoena, or a trial subpoena is obtained, delay the notification required under this Code section for a period not to exceed 90 days upon the execution of a written certification of the law enforcement agency, Attorney General, district attorney, or solicitor-general that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection means:

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

(B) Flight from prosecution;

(C) Destruction of or tampering with evidence;

(D) Intimidation of potential witnesses; or

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

(3) The law enforcement agency, the Attorney General, district attorney, or solicitor-general shall maintain a true copy of certification under subparagraph (B) of paragraph (1) of this subsection.

(4) Extensions of the delay of notification provided in this Code section of up to 90 days each may be granted by the court upon application or by certification by any law enforcement agency, the Attorney General, district attorney, or solicitor-general, but only in accordance with subsection (f) of this Code section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the law enforcement agency, the Attorney General, district attorney, or solicitor-general 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 a notice that:

(A) States with reasonable specificity the nature of the inquiry; and

(B) Informs such customer or subscriber:

(i) That information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that law enforcement agency, the Attorney General, district attorney, or solicitor-general, and the date on which the supplying or request took place;

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

(iii) Which law enforcement agency, the Attorney General, district attorney, solicitor-general, or court made the certification or determination to delay such notification; and

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

(f) Any law enforcement agency, the Attorney General, district attorney, or solicitor-general acting under this Code section, when it is not required to notify the subscriber or customer under paragraph (1) of subsection (b) of this Code section, or to the extent that it may delay such notice pursuant to subsection (e) of this Code section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in:

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

(2) Flight from prosecution;

(3) Destruction of or tampering with evidence;

(4) Intimidation of potential witnesses; or

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

(g)(1) Any records supplied pursuant to this Code section shall be accompanied by the affidavit of the custodian of the records or other qualified witness, stating in substance each of the following:

(A) The affiant is the duly authorized custodian of the records or other qualified witness and has authority to certify the records;

(B) Any copy of the records described in a subpoena, court order, or search warrant is a true copy, and the records were delivered to the attorney or the attorney´s representative;

(C) The records were prepared by the personnel of the business in the ordinary course of business at or near the time of the act, condition, or event;

(D) The sources of information and method and time of preparation were such as to indicate its trustworthiness;

(E) The identity of the records; and

(F) A description of the mode of preparation of the records.

(2) If the business has none of the records described, or only part thereof, the custodian of the records or other qualified witness shall so state in the affidavit required under paragraph (1) of this subsection.

(3) If the original records would be admissible in evidence if the custodian of the records or other qualified witness had been present and testified to the matters stated in the affidavit provided under paragraph (1) of this subsection, the copy of the records is admissible as evidence. The affidavit is admissible as evidence of the matters stated therein and the matters so stated are presumed true. When more than one person has knowledge of the facts, more than one affidavit may be made. The presumption established by this paragraph is a presumption affecting the burden of producing evidence.

(4) At the arraignment, but no later than 30 days prior to trial, a party intending to offer such evidence shall provide written notice of such intentions to the opposing party or parties. A motion opposing the admission of such evidence shall be made and determined by the court no later than ten days prior to trial. Failure of a party to file such motion prior to trial shall constitute a waiver of objection to said records and affidavit; however, the court, for cause shown, may grant relief from such waiver.

16-9-105.

(a) Any computer or other electronic equipment which is used or intended for use in any manner to commit a violation of Code Section 16-9-93, 16-9-101, 16-11-37, 16-12-100, 16-12-100.1, 16-12-100.2, 16-5-90, or 16-5-91 is contraband and forfeited to the state and no person shall have a property interest in it. Such property may be seized or detained in the same manner as provided in Code Section 16-13-49 and shall not be subject to replevin, conveyance, sequestration, or attachment.

(b) Within 60 days of the date of the seizure of proceeds or money pursuant to this Code section, the district attorney shall initiate forfeiture or other proceedings as provided in Code Section 16-13-49. An owner or interest holder, as defined by subsection (a) of Code Section 16-13-49, may establish as a defense to the forfeiture of such property which is subject to forfeiture under this Code section the applicable provisions of subsection (e) or (f) of Code Section 16-13-49. Proceeds or money which is forfeited pursuant to this Code section shall be disposed of and distributed as provided in Code Section 16-13-49.″

SECTION 4.

Article 2 of Chapter 5 of Title 17 of the Official Code of Georgia Annotated, relating to searches with warrants, is amended by inserting after Code Section 17-5-32 a new Code Section 17-5-33 to read as follows:

"17-5-33.

(a) As used in this Code section, the term:

(1) 'Adverse result' means a result that occurs when notification of the existence of a search warrant results in:

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

(B) A flight from prosecution;

(C) The destruction of or tampering with evidence;

(D) The intimidation of potential witnesses;

(E) Serious jeopardy to an investigation or undue delay of a trial.

(2) 'Business' means any lawful activity engaged in for profit or not for profit, whether organized as a corporation; a partnership, either general or limited; a sole proprietorship; an alien corporation which is required to register under the provisions of Code Section 16-14-15; or otherwise.

(3) 'Electronic communication services' and 'remote computing services' shall have the same meanings as provided in Code Section 16-9-100. This Code section shall not apply to business entities that do not provide those services to the general public.

(4) 'Properly served' means that a search warrant is issued and executed as provided for under the provisions of this article.

(b) The following provisions shall apply to any search warrant issued pursuant to this article allowing a search for records that are in the actual or constructive possession of an out-of-state business that provides electronic communication services or remote computing services to the general public where those records would reveal the identity of the customers using those services, data stored by, or on behalf of, the customer, the customer´s usage of those services, the recipient or destination of communications sent to or from those customers, or the content of those communications:

(1) When properly served with a search warrant issued by a Georgia court, an out-of-state business subject to this Code section shall provide to the applicant all records sought pursuant to that warrant within five business days of receipt, including those records maintained or located outside this state;

(2) Where the applicant makes a showing and the court finds that failure to produce records within five business days would cause an adverse result, the warrant may require production of records within fewer than five business days;

(3) A court may extend the time required for production of the records upon finding that the out-of-state business has shown good cause for that extension and that an extension of time would not cause an adverse result; and

(4) An out-of-state business seeking to quash the warrant must seek relief from the court that issued the warrant within the time required for production of records pursuant to this Code section. The issuing court shall hear and decide that motion no later than five court days after the motion is filed.

(c) A Georgia business that provides electronic communication services or remote computing services to the general public, when served with a warrant issued by another state to produce records that would reveal the identity of the customers using those services, data stored by, or on behalf of, the customer, the customer´s usage of those services, the recipient or destination of communications sent to or from those customers, or the content of those communications, shall produce those records as if that warrant had been issued by a Georgia court.

(d) No cause of action shall lie against any out-of-state or Georgia business subject to this Code section, its officers, employees, agents, or other specified persons for providing records, information, facilities, or assistance in accordance with the terms of a warrant issued pursuant to this chapter.″

SECTION 5.

Article 2 of Chapter 11 of Title 16 of the Official Code of Georgia Annotated, relating to offenses against public order, is amended in subsection (b) of Code Section 16-11-37, relating to terroristic threats, by striking the word "or" at the end of paragraph (2); by striking the period at the end of paragraph (3) and inserting in its place "; or"; and by adding at the end of subsection (b) a new paragraph (4) to read as follows:

″(4) He or she uses a computer, Internet chatroom, e-mail, or other electronic means to threaten to commit any crime of violence or to burn or damage property with the purpose of terrorizing another; causing the evacuation of a building, place of assembly, or facility of public transportation; otherwise causing serious public inconvenience; or in reckless disregard of the risk of causing such terror or inconvenience.″

SECTION 6.

Article 3 of Chapter 12 of Title 16 of the Official Code of Georgia Annotated, relating to obscenity and related offenses, is amended by striking subsection (g) of Code Section 16-12-100, relating to possession or control of any material which depicts a minor engaged in any sexually explicit conduct, and inserting in lieu thereof the following:

"(g)(1) Except as otherwise provided in ~~paragraphs (2) and (3)~~ paragraph (2) of this subsection, any person who violates a provision of this Code section shall be guilty of a felony and, upon conviction thereof, shall be punished by imprisonment for not less than five years nor more than 20 years and by a fine of not more than $100,000.00. In the event, however, that the person so convicted is a member of the immediate family of the victim, no fine shall be imposed.

~~(2) Any person who violates paragraph (8) of subsection (b) of this Code section shall be guilty of a misdemeanor.~~

~~(3)~~(2) Any person who violates subsection (c) of this Code section shall be guilty of a misdemeanor."

SECTION 7.

Said article is further amended by striking paragraph (2) of subsection (d) of Code Section 16-12-100.2, relating to computer pornography and child exploitation prevention, and inserting in lieu thereof the following:

"(2) Any person who violates paragraph (1) of this subsection shall be guilty of a ~~misdemeanor of a high and aggravated nature~~ felony and, upon conviction thereof, shall be punished by imprisonment for not less than five years nor more than 20 years and by a fine of not more than $100,000.00. In the event, however, that the person so convicted is a member of the immediate family of the victim, no fine shall be imposed."

SECTION 8.

Said article is further amended by inserting after Code Section 16-12-105 a new Code Section 16-12-106 to read as follows:

"16-12-106.

(a) 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 state within five business days of when the Internet service provider is notified by the Attorney General pursuant to subsection (g) of this Code section that child pornography items reside on or are accessible through its service.

(b) Nothing in this Code section 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.

(c) Notwithstanding any other provision of law to the contrary, any Internet service provider who violates subsection (a) of this Code section commits:

(1) A misdemeanor for a first offense punishable by a fine of $1,000.00;

(2) A misdemeanor of a high and aggravated nature for a second offense punishable by a fine of $5,000.00; or

(3) A felony for a third or subsequent offense punishable by a fine of $30,000.00 and imprisonment for a maximum of five years.

(d) The Attorney General shall have concurrent prosecutorial jurisdiction with a district attorney for violation of this Code section.

(e) 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 in writing to a superior court judge having jurisdiction 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 such an 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 (URL) providing access to such 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 such items constitute a violation of Code Sections 16-12-100, 16-12-100.1, and 16-12-100.2, relating to sexual exploitation of children;

(7) A proposed order of authorization for consideration by the judge;

(8) Contact information for the Office of the Attorney General, including the name, address, and telephone number of any deputy or agent authorized by the Attorney General to submit notification pursuant to subsection (g) of this Code section; and

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

(f) Upon consideration of an application, the court may enter an order, including an ex parte order, as requested, advising the Attorney General or district attorney that such items constitute probable cause for a violation of paragraph (1) of subsection (e) of Code Section 16-12-100.2 and that such items shall be removed or disabled from the Internet service provider´s service, and the court may include such other information as the court deems relevant and necessary.

(g)(1) The Attorney General shall have exclusive jurisdiction to notify Internet service providers under this Code section. The Attorney General shall initiate notification pursuant to this Code section if requested in writing by a district attorney who has provided the Attorney General with a copy of the application made pursuant to

subsection (e) of this Code section and a copy of the order issued pursuant to subsection (f) of this Code section or upon the issuance of an order based upon an application filed by the Attorney General.

(2) For purposes of this subsection, an Internet service provider or the person designated by the Internet service provider as provided for in subsection (h) of this Code section shall be notified in writing by the Attorney General within three business days of the Attorney General´s receipt of an order.

(3) The notice required under paragraph (2) of this subsection shall include the following information:

(A) A copy of the application made pursuant to subsection (e) of this Code section;

(B) A copy of the court order issued pursuant to subsection (f) of this Code section;

(C) 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; and

(D) Contact information for the Office of the 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.

(h) An Internet service provider may designate an agent to receive notification pursuant to subsection (g) of this Code section.

(i) As used in this Code section, the term:

(1) 'Child pornography' has the same meaning as provided in Code Section 16-12-100, relating to sexually explicit conduct with a minor.

(2) 'Internet' means the myriad computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide 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.

(3) 'Internet service provider' means a person who provides a service that enables users to access content, information, electronic mail, or other services offered over the Internet or a provider of electronic communication services as defined under Code Section 16-9-100.″

SECTION 9.

This Act shall become effective on the first day of the month following the month in which it is approved by the Governor or in which it becomes law without such approval.

SECTION 10.

All laws and parts of laws in conflict with this Act are repealed.