

The Senate Science and Technology Committee offered the following substitute to SB 425:

A BILL TO BE ENTITLED
AN ACT

1 To amend Article 9 of Chapter 9 of Title 16 of the Official Code of Georgia Annotated, the
2 "Georgia Computer Security Act of 2005," so as to enact "The Georgia Child, Family, and
3 School Communications Protection Act"; to provide a short title; to provide for definitions;
4 to create a service to protect child, family, and school communications; to provide conditions
5 for registration; to provide for a fee; to provide for procedures; to provide for verification
6 from the contents of the service; to prohibit the transmission of certain messages; to provide
7 for exceptions; to prohibit the release of certain information; to shield certain information
8 from public inspection; to provide for a penalty; to provide for civil actions; to provide for
9 related matters; to provide for an effective date; to repeal conflicting laws; and for other
10 purposes.

11 BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

SECTION 1.

12 Article 9 of Chapter 9 of Title 16 of the Official Code of Georgia Annotated, the "Georgia
13 Computer Security Act of 2005," is amended by designating the existing portion of such
14 article as Part 1 and by inserting at the end of such article the following:
15

"Part 2

16
17 16-9-170.

18 This part shall be known and may be cited as the 'The Georgia Child, Family, and School
19 Communications Protection Act.'

20 16-9-171.

21 As used in this part, the term:

22 (1) 'Contact point' means any electronic identification to which messages can be sent,
23 including any of the following:

- 1 (A) An instant message identity;
2 (B) A wireless telephone, a personal digital assistant, a pager number, or any other
3 similar wireless communication device;
4 (C) A facsimile number;
5 (D) An electronic mail address; or
6 (E) Other electronic addresses subject to rules promulgated under this part by the
7 department.

8 (2) 'Division' means the Division of Family and Children Services of the Department of
9 Human Resources.

10 (3) 'Internet domain name' means a globally unique, hierarchical reference to an Internet
11 host or service, assigned through centralized Internet authorities, comprising a series of
12 character strings separated by periods, with the right-most string specifying the top of the
13 hierarchy.

14 (4) 'Minor' means an individual under the age of 18 years.

15 (5) 'Person' means an individual, corporation, association, partnership, or any other legal
16 entity.

17 (6) 'Service' means the Georgia Child, Family, and School Communications Protection
18 Service created under Code Section 16-9-172.

19 16-9-172.

20 (a) The division shall establish and operate, or contract with a qualified third party to
21 establish and operate, the Georgia Child, Family, and School Communications Protection
22 Service. The division or a third party administrator shall establish procedures to prevent
23 the use or disclosure of protected contact points as required under Code Section 16-9-174.

24 (b) A parent, guardian, individual, or an entity under subsection (d) of this Code section
25 who is responsible for a contact point to which a minor may have access or which is used
26 by a household in which a minor is present may register that contact point with the
27 department under rules promulgated by the division. The division shall establish
28 procedures to ensure that a registrant meets the requirements of this subsection.

29 (c) A registration under this Code section shall be for not more than three years. If the
30 contact point is established for a specific minor, the registration expires when the minor
31 reaches 18 years of age. A registration can be revoked or renewed by the registrant upon
32 notification to the division.

33 (d) Schools and other institutions or entities primarily serving minor children may register
34 one or more contact points with the division. An entity under this subsection may make
35 one registration for all contact points of the entity, and the registration may include the
36 entity's Internet domain name under rules promulgated by the division.

1 (e) No fee or charge shall be assessed or incurred by a person registering a contact point
2 under this part.

3 (f) The division shall establish a mechanism for senders to verify compliance with the
4 service.

5 (g) A person desiring to send a message described in Code Section 16-9-173 shall pay the
6 division a fee for access to the mechanism required under subsection (f) of this Code
7 section. The fee required under this subsection shall be set by the division. The fee shall
8 not exceed 1¢ per contact point. The mechanism to verify compliance under subsection
9 (f) of this Code section and the fee required under this subsection shall be established under
10 rules promulgated by the division.

11 (h) The service shall be fully operational not later than December 1, 2006.

12 16-9-173.

13 (a) Except as otherwise provided in this Code section, a person shall not send, cause to be
14 sent, or conspire with a third party to send a message to a contact point that has been
15 registered with the service for at least 30 calendar days if the primary purpose of the
16 message is to advertise or induce the sale of a product or service that a minor is prohibited
17 by law from purchasing, viewing, possessing, participating in, or otherwise receiving.

18 (b) A person desiring to send a message described in subsection (a) of this Code section
19 shall use the mechanism created under subsection (f) of Code Section 16-9-172 to ensure
20 compliance with this part.

21 (c) Senders that, in good faith, use the mechanism created under subsection (f) of Code
22 Section 16-9-172 to remove all registered contact points at least every 30 days from their
23 sending lists shall receive a safe harbor from criminal prosecution and civil actions under
24 this part for inadvertent violations of this part during the period in which the mechanism
25 was used.

26 (d) Except as otherwise provided in subsection (h) of this Code section, the consent to
27 receive the message is not a defense to a violation of this Code section.

28 (e) A person does not violate this part because the person is an intermediary between the
29 sender and recipient in the transmission of an electronic message that violates this part or
30 unknowingly provides transmission of electronic messages over the person's computer
31 network or facilities that violate this part.

32 (f) The sending of a message described in subsection (a) of this Code section is prohibited
33 only if it is otherwise a crime for the minor to purchase, view, possess, participate in, or
34 otherwise receive the product or service.

35 (g) Senders shall be considered on notice of jurisdiction over contact points that have been
36 registered for at least 30 days with the service. Sending a message to an address registered

1 for at least 30 calendar days with the child, family, and school communication protection
2 service shall subject the sender to the state's long arm jurisdiction.

3 (h) The sending of a message described in subsection (a) of this Code section shall not be
4 prohibited if, prior to sending the message, the sender has obtained from an adult whose
5 age the sender has verified a statement consenting to receive the message at a contact point
6 which such adult has verified as being such adult's contact point. To comply with this
7 subsection, the sender shall:

8 (1) Verify that the person making the affirmative statement is of legal age by inspecting
9 in a face-to-face meeting a valid photo identification issued by a governmental agency;

10 (2) Obtain a written consent form signed by the recipient stating that the recipient has
11 consented to receive the type of message described in subsection (a) of this Code section.
12 The sender shall retain the consent form on record and shall make it available as provided
13 in paragraph (4) of this subsection;

14 (3) Include in all messages sent pursuant to this subsection a statement that the recipient
15 may rescind his or her consent and provide an opportunity for the recipient to opt not to
16 receive future messages; and

17 (4) Notify the division that the sender intends to send messages as provided in this
18 subsection. The division may implement procedures to audit the sender's records to
19 verify that the sender is in compliance with this subsection.

20 16-9-174.

21 (a) A person shall not release to another person information concerning persons or provide
22 access to contact points or other information contained on the service except as provided
23 by this part.

24 (b) A person shall not sell or use the contents of the service for any reason other than to
25 meet the requirements of this part.

26 (c) A person shall not access or attempt to access the service except as provided by this
27 part.

28 (d) Records and documents of the service created under this part are not subject to public
29 inspection pursuant to Article 4 of Chapter 18 of Title 50.

30 16-9-175.

31 A violation of this part shall be a computer crime and a felony punishable by incarceration
32 up to five years or a fine not to exceed \$200,000.00, or both. Each violation of this part
33 shall constitute a separate offense.

1 16-9-176.

2 (a) A civil action based on a violation of this part may be brought:

3 (1) By an authorized individual or the registrant of the contact point on behalf of a minor
4 who has received a message in violation of this part;

5 (2) By a person through whose facilities the message was transmitted in violation of this
6 part; or

7 (3) By the Attorney General against a person who has violated this part.

8 (b) In each action brought under this Code section, the prevailing party may be awarded
9 reasonable attorney fees.

10 (c) A person bringing an action under this Code section may recover:

11 (1) Actual damages, including reasonable attorney fees; or

12 (2) In lieu of actual damages, the lesser of \$5,000.00 per each message received by a
13 recipient or transmitted or \$250,000.00 for each day that the violation occurs.

14 (d) It shall be an affirmative defense to a civil action based on a violation of this part
15 brought by an individual who registered a contact point if the sender proves that the
16 individual affirmatively, expressly, and directly consented, and did not subsequently revoke
17 such consent, to receive messages from the particular sender to the registered contact point.
18 Such consent shall not be a defense to a criminal or civil action brought by the Attorney
19 General or by a person through whose facilities the message was transmitted in violation
20 of this part.

21 (e) If the Attorney General has reason to believe that a person has violated this part, the
22 Attorney General may investigate the business transactions of that person. The Attorney
23 General may require that person to appear, at a reasonable time and place, to give
24 information under oath and to produce such documents and evidence necessary to
25 determine whether the person is in compliance with the requirements of this part."

26 **SECTION 2.**

27 Said article is further amended by striking in its entirety Code Section 16-9-150, relating to
28 a short title, and inserting in lieu thereof the following:

29 "16-9-150.

30 This ~~article~~ part shall be known and may be cited as the 'Georgia Computer Security Act
31 of 2005.'"

32 **SECTION 3.**

33 Said article is further amended by striking in its entirety Code Section 16-9-151, relating to
34 definitions, and inserting in lieu thereof the following:

1 "16-9-151.

2 As used in this ~~chapter~~ part, the term:

3 (1) 'Advertisement' means a communication, the primary purpose of which is the
4 commercial promotion of a commercial product or service, including content on an
5 Internet website operated for a commercial purpose.

6 (2) 'Authorized user' with respect to a computer, means a person who owns or is
7 authorized by the owner or lessee to use the computer.

8 (3) 'Cause to be copied' means to distribute or transfer computer software or any
9 component thereof. Such term shall not include providing:

10 (A) Transmission, routing, provision of intermediate temporary storage, or caching of
11 software;

12 (B) A storage medium, such as a compact disk, website, or computer server, through
13 which the software was distributed by a third party; or

14 (C) An information location tool, such as a directory, index, reference, pointer, or
15 hypertext link, through which the user of the computer located the software.

16 (4) 'Computer software' means a sequence of instructions written in any programming
17 language that is executed on a computer. Such term shall not include a text or data file,
18 a web page, or a data component of a web page that is not executable independently of
19 the web page.

20 (5) 'Computer virus' means a computer program or other set of instructions that is
21 designed to degrade the performance of or disable a computer or computer network and
22 is designed to have the ability to replicate itself on other computers or computer networks
23 without the authorization of the owners of those computers or computer networks.

24 (6) 'Consumer' means an individual who resides in this state and who uses the computer
25 in question primarily for personal, family, or household purposes.

26 (7) 'Damage' means any significant impairment to the integrity or availability of data,
27 software, a system, or information.

28 (8) 'Execute,' when used with respect to computer software, means the performance of
29 the functions or the carrying out of the instructions of the computer software.

30 (9) 'Intentionally deceptive' means any of the following:

31 (A) By means of an intentionally and materially false or fraudulent statement;

32 (B) By means of a statement or description that intentionally omits or misrepresents
33 material information in order to deceive the consumer; or

34 (C) By means of an intentional and material failure to provide any notice to an
35 authorized user regarding the download or installation of software in order to deceive
36 the consumer.

1 (10) 'Internet' means the global information system that is logically linked together by
2 a globally unique address space based on the Internet Protocol or its subsequent
3 extensions; that is able to support communications using the Transmission Control
4 Protocol/Internet Protocol suite, its subsequent extensions, or other Internet Protocol
5 compatible protocols; and that provides, uses, or makes accessible, either publicly or
6 privately, high level services layered on the communications and related infrastructure
7 described in this paragraph.

8 (11) 'Person' means any individual, partnership, corporation, limited liability company,
9 or other organization, or any combination thereof.

10 (12) 'Personally identifiable information' means any of the following:

11 (A) A first name or first initial in combination with a last name;

12 (B) Credit or debit card numbers or other financial account numbers;

13 (C) A password or personal identification number required to access an identified
14 financial account;

15 (D) A social security number; or

16 (E) Any of the following information in a form that personally identifies an authorized
17 user:

18 (i) Account balances;

19 (ii) Overdraft history;

20 (iii) Payment history;

21 (iv) A history of websites visited;

22 (v) A home address;

23 (vi) A work address; or

24 (vii) A record of a purchase or purchases."

25 **SECTION 4.**

26 Said article is further amended by striking in its entirety subsection (b) of Code Section
27 16-9-152, relating to spyware, browsers, hijacks, and other software prohibited, and inserting
28 in lieu thereof the following:

29 "(b) Nothing in this Code section shall apply to any monitoring of, or interaction with, a
30 user's Internet or other network connection or service, or a protected computer, by a
31 telecommunications carrier, cable operator, computer hardware or software provider, or
32 provider of information service or interactive computer service for network or computer
33 security purposes, diagnostics, technical support, repair, network management, network
34 maintenance, authorized updates of software or system firmware, authorized remote system
35 management, or detection or prevention of the unauthorized use of or fraudulent or other

1 illegal activities in connection with a network, service, or computer software, including
 2 scanning for and removing software proscribed under this ~~article~~ part."

3 SECTION 5.

4 Said article is further amended by striking in its entirety subsection (b) of Code Section
 5 16-9-153, relating to e-mail virus distribution, denial of service attacks, and other conduct
 6 prohibited, and inserting in lieu thereof the following:

7 "(b) Nothing in this Code section shall apply to any monitoring of, or interaction with, a
 8 user's Internet or other network connection or service, or a protected computer, by a
 9 telecommunications carrier, cable operator, computer hardware or software provider, or
 10 provider of information service or interactive computer service for network or computer
 11 security purposes, diagnostics, technical support, repair, network management, network
 12 maintenance, authorized updates of software or system firmware, authorized remote system
 13 management, or detection or prevention of the unauthorized use of or fraudulent or other
 14 illegal activities in connection with a network, service, or computer software, including
 15 scanning for and removing software proscribed under this ~~article~~ part."

16 SECTION 6.

17 Said article is further amended by striking in its entirety subsection (b) of Code Section
 18 16-9-154, relating to inducement to install, copy, or execute software through
 19 misrepresentation prohibited, and inserting in lieu thereof the following:

20 "(b) Nothing in this Code section shall apply to any monitoring of, or interaction with, a
 21 user's Internet or other network connection or service, or a protected computer, by a
 22 telecommunications carrier, cable operator, computer hardware or software provider, or
 23 provider of information service or interactive computer service for network or computer
 24 security purposes, diagnostics, technical support, repair, network management, network
 25 maintenance, authorized updates of software or system firmware, authorized remote system
 26 management, or detection or prevention of the unauthorized use of or fraudulent or other
 27 illegal activities in connection with a network, service, or computer software, including
 28 scanning for and removing software proscribed under this ~~article~~ part."

29 SECTION 7.

30 Said article is further amended by striking in its entirety Code Section 16-9-155, relating to
 31 penalties, and inserting in lieu thereof the following:

32 "16-9-155.

33 (a) Any person who violates the provisions of paragraph (2) of Code Section 16-9-152,
 34 ~~subparagraph (A), (B), or (C) of paragraph (1) of subsection (a)~~ (a)(1)(A), (a)(1)(B), or

1 (a)(1)(C) of Code Section 16-9-153, or paragraph (2) of subsection (a) of Code Section
 2 16-9-153 shall be guilty of a felony and, upon conviction thereof, shall be sentenced to
 3 imprisonment for not less than one nor more than ten years or a fine of not more than \$3
 4 million, or both.

5 (b) The Attorney General may bring a civil action against any person violating this ~~article~~
 6 part to enforce the penalties for the violation and may recover any or all of the following:

- 7 (1) A civil penalty of up to \$100.00 per violation of this ~~article~~ part, or up to \$100,000.00
- 8 for a pattern or practice of such violations;
- 9 (2) Costs and reasonable attorney's fees; and
- 10 (3) An order to enjoin the violation.

11 (c) In the case of a violation of subparagraph ~~(B)~~ of paragraph ~~(1)~~ of subsection ~~(a)~~
 12 (a)(1)(B) of Code Section 16-9-153 that causes a telecommunications carrier to incur costs
 13 for the origination, transport, or termination of a call triggered using the modem of a
 14 customer of such telecommunications carrier as a result of such violation, the
 15 telecommunications carrier may bring a civil action against the violator to recover any or
 16 all of the following:

- 17 (1) The charges such carrier is obligated to pay to another carrier or to an information
- 18 service provider as a result of the violation, including, but not limited to, charges for the
- 19 origination, transport, or termination of the call;
- 20 (2) Costs of handling customer inquiries or complaints with respect to amounts billed for
- 21 such calls;
- 22 (3) Costs and reasonable attorney's fees; and
- 23 (4) An order to enjoin the violation.

24 (d) An Internet service provider or software company that expends resources in good faith
 25 assisting consumers or business entities harmed by a violation of this chapter, or a
 26 trademark owner whose mark is used to deceive consumers or business entities in violation
 27 of this chapter, may enforce the violation and may recover any or all of the following:

- 28 ~~(1)(A)~~ Statutory damages of not more than \$100.00 per violation of this ~~article~~ part, or
- 29 up to \$1 million for a pattern or practice of such violations;
- 30 (2) Costs and reasonable attorney's fees; and
- 31 (3) An order to enjoin the violation."

32 SECTION 8.

33 Said article is further amended by striking in its entirety Code Section 16-9-156, relating to
 34 exceptions, and inserting in lieu thereof the following:

35 "(a) For the purposes of this Code section, the term 'employer' includes a business entity's
 36 officers, directors, parent corporation, subsidiaries, affiliates, and other corporate entities

1 under common ownership or control within a business enterprise. No employer may be
 2 held criminally or civilly liable under this ~~article~~ part as a result of any actions taken:

3 (1) With respect to computer equipment used by its employees, contractors,
 4 subcontractors, agents, leased employees, or other staff which the employer owns, leases,
 5 or otherwise makes available or allows to be connected to the employer's network or
 6 other computer facilities; or

7 (2) By employees, contractors, subcontractors, agents, leased employees, or other staff
 8 who misuse an employer's computer equipment for an illegal purpose without the
 9 employer's knowledge, consent, or approval.

10 (b) No person shall be held criminally or civilly liable under this ~~article~~ part when its
 11 protected computers have been used by unauthorized users to violate this ~~article~~ part or
 12 other laws without such person's knowledge, consent, or approval.

13 (c) A manufacturer or retailer of computer equipment shall not be liable under this Code
 14 section, criminally or civilly, to the extent that the manufacturer or retailer is providing
 15 third-party branded software that is installed on the computer equipment that the
 16 manufacturer or retailer is manufacturing or selling."

17 **SECTION 9.**

18 Said article is further amended by striking in its entirety Code Section 16-9-157, relating to
 19 legislative findings and preemption, and inserting in lieu thereof the following:

20 "16-9-157.

21 The General Assembly finds that this ~~article~~ part is a matter of state-wide concern. This
 22 ~~article~~ part supersedes and preempts all rules, regulations, codes, ordinances, and other
 23 laws adopted by any county, municipality, consolidated government, or other local
 24 governmental agency regarding spyware and notices to consumers from computer software
 25 providers regarding information collection."

26 **SECTION 10.**

27 This Act shall become effective upon its approval by the Governor or upon its becoming law
 28 without such approval.

29 **SECTION 11.**

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