The Senate Science and Technology Committee offered the following substitute to SB 127:

A BILL TO BE ENTITLED
AN ACT

1   To amend Chapter 9 of Title 16 of the Official Code of Georgia Annotated, relating to
2   forgery and fraudulent practices, so as to enact the "Georgia Computer Security Act of
3   2005"; to provide a short title; to provide definitions; to prohibit certain deceptive acts and
4   practices with regard to computers; to require certain notices be given prior to certain
5   software or programs being loaded onto certain computers; to require certain functions be
6   available in certain software; to provide for certain exceptions; to provide for civil and
7   criminal penalties; to provide for recovery of certain damages; to provide for applicability;
8   to provide for related matters; to amend Code Section 16-14-3 of the Official Code of
9   Georgia Annotated, relating to the "Georgia RICO (Racketeer Influenced and Corrupt
10 Organizations) Act," so as to add violations concerning deceptive acts or practices to the list
11 of predicate acts; to provide for related matters; to repeal conflicting laws; and for other
12 purposes.

13   BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

14   **SECTION 1.**
15 Chapter 9 of Title 16 of the Official Code of Georgia Annotated, relating to forgery and
16 fraudulent practices, is amended by adding a new Article 9 to read as follows:

17   "ARTICLE 9

18   16-9-150.
19   This chapter shall be known and may be cited as the 'Georgia Computer Security Act of
20   2005.'

21   16-9-151.
22   As used in this chapter, the term:

1   (1) 'Computer' means an electronic, magnetic, optical, electrochemical, or other high
2   speed data processing device performing logical, arithmetic, or storage functions, and
3   includes any data storage facility or communications facility directly related to or
4   operating in conjunction with such device, but such term does not include an automated
5   typewriter or typesetter, a portable hand-held calculator, or other similar device.
6   (2) 'Disable' means, with respect to an information collection program, to permanently
7   prevent such program from executing any of the functions described in paragraph (3) of
8   this Code section that such program is otherwise capable of executing by removing,
9   deleting, or disabling the program unless the owner of a protected computer takes a
10   subsequent affirmative action to enable the execution of such functions.
11   (3) 'Information collection program' means computer software that:
12   (A) Collects personally identifiable information and sends such information to a person
13   other than the owner or authorized user of the computer or uses such information to
14   deliver advertising to or display advertising on the computer; or
15   (B) Collects information regarding the webpages accessed using the computer and uses
16   such information to deliver advertising to or display advertising on the computer.
17   (4) 'Internet' means collectively the myriad of computer and telecommunications
18   facilities, including equipment and operating software, which comprise the
19   interconnected world-wide network of networks that employ the Transmission Control
20   Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol,
21   to communicate information of all kinds by wire or radio.
22   (5) 'Personally identifiable information' means the following information, to the extent
23   only that such information allows a living individual to be identified from that
24   information:
25   (A) First and last name of an individual;
26   (B) A home or other physical address of an individual, including street name, name of
27   a city or town, and ZIP Code;
28   (C) An electronic mail address;
29   (D) A telephone number;
30   (E) A social security number, tax identification number, passport number, driver´s
31   license number, or any other government issued identification number;
32   (F) A credit card number;
33   (G) Any access code, password, or account number, other than an access code or
34   password transmitted by an owner or authorized user of a protected computer to the
35   intended recipient to register for, or log onto, a webpage or other Internet service or a
36   network connection or service of a subscriber that is protected by an access code or
37   password; and

1   (H) Date of birth, birth certificate number, or place of birth of an individual, except in

2   the case of a date of birth transmitted or collected for the purpose of compliance with

3   the law.

4   (6) 'Protected computer" means a computer which, at the time of an alleged violation of

5   this article involving that computer, is located within the geographic boundaries of this

6   state.

7   (7) 'Webpage' means a location, with respect to the World Wide Web, that has a single

8   uniform resource locator or another single location with respect to the Internet.

9   16-9-152.

10   (a) It shall be an unlawful deceptive act or practice for any person who is not the owner

11   or authorized user of a protected computer to engage in any of the following acts or

12   practices with respect to a protected computer:

13   (1) Taking control of the computer by:

14   (A) Utilizing such computer to send unsolicited information or material from the

15   protected computer to others;

16   (B) Diverting the Internet browser of the computer, or similar program of the computer

17   used to access and navigate the Internet:

18   (i) Without authorization of the owner or authorized user of the computer; and

19   (ii) Away from the site the user intended to view, to one or more other webpages,

20   such that the user is prevented from viewing the content at the intended webpage,

21   unless such diverting is otherwise authorized;

22   (C) Accessing or using the modem or Internet connection or service for the computer

23   and thereby causing damage to the computer or causing the owner or authorized user

24   to incur unauthorized financial charges;

25   (D) Using the computer as part of an activity performed by a group of computers that

26   causes damage to another computer; or

27   (E) Delivering advertisements that a user of the computer cannot close without turning

28   off the computer or closing all sessions of the Internet browser for the computer;

29   (2) Modifying settings related to use of the computer or to the computer´s access to or

30   use of the Internet by altering:

31   (A) The webpage that appears when the owner or authorized user launches an Internet

32   browser or similar program used to access and navigate the Internet;

33   (B) The default provider used to access or search the Internet, or other existing Internet

34   connections settings;

35   (C) A list of bookmarks used by the computer to access webpages; or

1   (D) Security or other settings of the computer that protect information about the owner

2   or authorized user for the purposes of causing damage or harm to the computer or

3   owner or user;

4   (3) Collecting personally identifiable information through the use of a keystroke logging

5   function;

6   (4) Inducing the owner or authorized user to install a computer software component onto

7   the computer, or preventing reasonable efforts to block the installation or execution of,

8   or to disable, a computer software component by:

9   (A) Presenting the owner or authorized user with an option to decline installation of

10   a software component such that, when the option is selected by the owner or authorized

11   user, the installation nevertheless proceeds; or

12   (B) Causing a computer software component that the owner or authorized user has

13   properly removed or disabled to reinstall or reactivate automatically on the computer;

14   (5) Misrepresenting that installing a separate software component or providing log-in and

15   password information is necessary for security or privacy reasons, or that installing a

16   separate software component is necessary to open, view, or play a particular type of

17   content;

18   (6) Inducing the owner or authorized user to install or execute computer software by

19   misrepresenting the identity or authority of the person or entity providing the computer

20   software to the owner or user;

21   (7) Inducing the owner or authorized user to provide personally identifiable, password,

22   or account information to another person:

23   (A) By misrepresenting the identity of the person seeking the information; or

24   (B) Without the authority of the intended recipient of the information;

25   (8) Removing, disabling, or rendering inoperative a security, antispyware, or antivirus

26   technology installed on the computer; or

27   (9) Installing or executing on the computer one or more additional computer software

28   components with the intent of causing a person to use such components in a way that

29   violates any other provision of this chapter.

30   (b) Except as otherwise provided in this Code section, it shall be unlawful for any person:

31   (1) To transmit to a protected computer, which is not owned by such person and for

32   which such person is not an authorized user, any information collection program, unless:

33   (A) Such information collection program provides notice in accordance with

34   subsection (c) of this Code section before execution of any of the information collection

35   functions of the program; and

36   (B) Such information collection program includes the functions required under

37   subsection (d) of this Code section; or

1   (2)   To execute any information collection program installed on such a protected

2   computer unless:

3   (A) Before execution of any of the information collection functions of the program, the

4   owner or an authorized user of the protected computer has consented to such execution

5   pursuant to notice in accordance with subsection (c) of this Code section; and

6   (B)   Such information collection program includes the functions required under

7   subsection (d) of this Code section.

8   (c)(1) Notice in accordance with this subsection with respect to an information collection

9   program is clear and conspicuous notice in plain language that meets all of the following

10   requirements:

11   (A) The notice clearly distinguishes such notice from any other information visually

12   presented contemporaneously on the protected computer;

13   (B)   The notice contains one of the following statements, as applicable, or a

14   substantially similar statement:

15   (i) With respect to an information collection program described in subparagraph (A)

16   of paragraph (3) of Code Section 16-9-151: 'This program will collect and transmit

17   information about you. Do you accept?';

18   (ii) With respect to an information collection program described in subparagraph (B)

19   of paragraph (3) of Code Section 16-9-151: 'This program will collect information

20   about webpages you access and will use that information to display advertising on

21   your computer. Do you accept?'; or

22   (iii) With respect to an information collection program that performs the actions

23   described in both subparagraphs (A) and (B) of paragraph (3) of Code Section

24   16-9-151: 'This program will collect and transmit information about you and your

25   computer use and will collect information about webpages you access and use that

26   information to display advertising on your computer. Do you accept?';

27   (C) The notice provides for the user:

28   (i) To grant or deny consent referred to in subsection (b) of this Code section by

29   selecting an option to grant or deny such consent; and

30   (ii) To abandon or cancel the transmission or execution referred to in subsection (b)

31   of this Code section without granting or denying such consent;

32   (D) The notice provides an option for the user to select to display on the computer,

33   before granting or denying consent using the option required under subparagraph (C)

34   of this paragraph, a clear description of:

35   (i) The types of information to be collected and sent, if any, by the information

36   collection program;

37   (ii) The purpose for which such information is to be collected and sent; and

1   (iii) In the case of an information collection program that first executes any of the

2   information collection functions of the program together with the first execution of

3   other computer software, the identity of any such software that is an information

4   collection program; and

5   (E) The notice provides for concurrent display of the information required under

6   subparagraphs (B) and (C) of this paragraph and the option required under

7   subparagraph (D) of this paragraph until the user:

8   (i) Grants or denies consent using the option required under division (i) of

9   subparagraph (C) of this paragraph;

10   (ii) Abandons or cancels the transmission or execution pursuant to division (ii) of

11   subparagraph (C) of this paragraph; or

12   (iii) Selects the option required under subparagraph (D) of this paragraph.

13   (2) In the case in which multiple information collection programs are provided to the

14   protected computer together, or as part of a suite of functionally related software, the

15   notice requirements of subparagraphs (1) and (2) of subsection (b) of this Code section

16   may be met by providing, before execution of any of the information collection functions

17   of the programs, clear and conspicuous notice in plain language in accordance with

18   paragraph (1) of this subsection by means of a single notice that applies to all such

19   information collection programs, except that such notice shall provide the option under

20   subparagraph (D) of paragraph (1) of this subsection with respect to each such

21   information collection program.

22   (3) If an owner or authorized user has granted consent to execution of an information

23   collection program pursuant to a notice in accordance with this Code section:

24   (A) No subsequent such notice is required, except as provided in subparagraph (B) of

25   this paragraph; and

26   (B) The person who transmitted the program shall provide another notice in accordance

27   with this subsection and obtain consent before such program may be used to collect or

28   send information of a type or for a purpose that is materially different from, and outside

29   the scope of, the type or purpose set forth in the initial or any previous notice.

30 (d) The functions required under this Code section to be included in an information

31 collection program that executes any information collection functions with respect to a

32 protected computer are as follows:

33   (1) Disabling function. With respect to any information collection program, a function

34   of the program that allows a user of the program to remove the program or disable

35   operation of the program with respect to such protected computer by a function that:

36   (A) Is easily identifiable to a user of the computer; and

1   (B) Can be performed without undue effort or knowledge by the user of the protected

2   computer; and

3   (2) Identity function. With respect only to an information collection program that uses

4   information collected in the manner described in subparagraph (A) or (B) of paragraph

5   (3) of Code Section 16-9-151, a function of the program that provides that each display

6   of an advertisement directed or displayed using such information when the owner or

7   authorized user is accessing a webpage or online location other than that of the provider

8   of the software is accompanied by the name of the information collection program, a

9   logogram or trademark used for the exclusive purpose of identifying the program, or a

10   statement or other information sufficient to clearly identify the program.

11   (e) A telecommunications carrier, a provider of information service or interactive

12   computer service, a cable operator, or a provider of transmission capability shall not be

13   liable, criminally or civilly, under this Code section to the extent that the carrier, operator,

14   or provider:

15   (1) Transmits, routes, hosts, stores, or provides connections for an information collection

16   program through a system or network controlled or operated by or for the carrier,

17   operator, or provider; or

18   (2) Provides an information location tool, such as a directory, index, reference, pointer,

19   or hypertext link, through which the owner or user of a protected computer locates an

20   information collection program.

21   (f)   This Code section shall not apply to:

22   (1) Any act taken by a law enforcement agent in the performance of official duties; or

23   (2) The transmission or execution of an information collection program in compliance

24   with a law enforcement, investigatory, national security, or regulatory agency or

25   department of the United States or any state in response to a request or demand made

26   under authority granted to that agency or department, including a warrant issued under

27   the Federal Rules of Criminal Procedure, an equivalent state warrant, a court order, or

28   other lawful process.

29   (g) This Code section shall not apply to:

30   (1) Any monitoring of or interaction with a subscriber´s Internet or other network

31   connection or service, or a protected computer, by a telecommunications carrier, cable

32   operator, computer hardware or software provider, or provider of information service or

33   interactive computer service, to the extent that such monitoring or interaction is for

34   network or computer security purposes, diagnostics, technical support, or repair, or for

35   the detection or prevention of fraudulent activities; or

1   (2) A discrete interaction with a protected computer by a provider of computer software

2   solely to determine whether the user of the computer is authorized to use such software

3   that occurs upon:

4   (A) Initialization of the software; or

5   (B) An affirmative request by the owner or authorized user for an update of, addition

6   to, or technical service for the software.

7 (h) No provider of computer software or of interactive computer service may be held

8 liable, criminally or civilly, under this Code section on account of any action voluntarily

9 taken, or service provided, in good faith to remove or disable a program used to violate this

10 Code section that is installed on a computer of a customer of such provider, if such

11 provider notifies the customer and obtains the consent of the customer before undertaking

12 such action or providing such service.

13 (i) 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 equipment the manufacturer or retailer

16 is manufacturing or selling.

17 (j) For the purposes of this Code section, the term 'employer' includes a business´s officers,

18 directors, parent corporation, subsidiaries, affiliates, and other corporate entities under

19 common ownership or control within an enterprise. No employer may be held liable

20 criminally or civilly under this article on account of any actions taken:

21   (1) With respect to computer equipment used by its employees, contractors,

22   subcontractors, agents, leased employees, or other staff where the employer owns, leases,

23   or otherwise makes available, or which employer allows to be connected to the

24   employer´s network or other computer facilities; or

25   (2) By employees, contractors, subcontractors, agents, leased employees, or other staff

26   who misuse an employer´s computer equipment for an illegal purpose without the

27   employer´s knowledge, consent, or approval.

28 (k) No person shall be liable criminally or civilly under this article when its protected

29 computers have been used by unauthorized persons to violate this Code section or other

30 laws without such person´s knowledge, consent, or approval.

31 16-9-153.

32 Any person that violates the provisions of Code Section 16-9-152 shall be guilty of a felony

33 and, upon conviction thereof, shall be sentenced to imprisonment for not less than one nor

34 more than ten years or a fine of not more than $3 million, or both.

1   16-9-154.

2   Any person who suffers personal, property, or economic damages by reason of a violation

3   of Code Section 16-9-152 may initiate a civil action for and recover the greater of:

4   (1) Five thousand dollars plus expenses of litigation and reasonable attorney´s fees;

5   (2) Liquidated damages of $1,000.00 for each violation of Code Section 16-9-152 up to

6   a limit of $2 million per incident, plus expenses of litigation and reasonable attorney´s

7   fees; or

8   (3) Actual damages, plus expenses of litigation and reasonable attorney´s fees.

9   16-9-155.

10   The provisions of this article shall not be construed to limit or preclude the applicability

11   of any other provision of criminal or civil law of this state which presently applies or may

12   in the future apply to any transaction or course of conduct which violates Code Section

13   16-9-152 unless such provision is clearly and irresolvably in conflict with the terms of this

14   article."

15   **SECTION 2.**

16   Code Section 16-14-3 of the Official Code of Georgia Annotated, relating to definitions

17   relating to the "Georgia RICO (Racketeer Influenced and Corrupt Organizations) Act," by

18   striking the word "or" at the end of division (9)(A)(xxxvii), by striking the period at the end

19   of division (9)(A)(xxxviii) and inserting in lieu thereof "; or", and by adding a new division

20   (9)(A)(xxxix) to read as follows:

21   "(xxxix) Code Section 16-9-152, relating to deceptive acts or practices with regard

22   to protected computers."

23   **SECTION 3.**

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