

The House Committee on Science and Technology offers 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 provide a short title; to provide definitions; to
3 prohibit certain conduct with regard to computers and computer software; to provide for
4 penalties for violations; to provide exceptions; to provide for certain civil remedies for
5 violations; to provide for preemption; to provide for related matters; to provide an effective
6 date; to repeal conflicting laws; and for other purposes.

7 BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

8 **SECTION 1.**

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

11 "ARTICLE 9

12 16-9-150.

13 This article shall be known and may be cited as the 'Georgia Computer Security Act of
14 2005.'

15 16-9-151.

16 As used in this chapter, the term:

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

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

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

- 1 (A) Transmission, routing, provision of intermediate temporary storage, or caching of
2 software;
- 3 (B) A storage medium, such as a compact disk, website, or computer server, through
4 which the software was distributed by a third party; or
- 5 (C) An information location tool, such as a directory, index, reference, pointer, or
6 hypertext link, through which the user of the computer located the software.
- 7 (4) 'Computer software' means a sequence of instructions written in any programming
8 language that is executed on a computer. Such term shall not include a text or data file,
9 a web page, or a data component of a web page that is not executable independently of
10 the web page.
- 11 (5) 'Computer virus' means a computer program or other set of instructions that is
12 designed to degrade the performance of or disable a computer or computer network and
13 is designed to have the ability to replicate itself on other computers or computer networks
14 without the authorization of the owners of those computers or computer networks.
- 15 (6) 'Consumer' means an individual who resides in this state and who uses the computer
16 in question primarily for personal, family, or household purposes.
- 17 (7) 'Damage' means any significant impairment to the integrity or availability of data,
18 software, a system, or information.
- 19 (8) 'Execute,' when used with respect to computer software, means the performance of
20 the functions or the carrying out of the instructions of the computer software.
- 21 (9) 'Intentionally deceptive' means any of the following:
- 22 (A) By means of an intentionally and materially false or fraudulent statement;
- 23 (B) By means of a statement or description that intentionally omits or misrepresents
24 material information in order to deceive the consumer; or
- 25 (C) By means of an intentional and material failure to provide any notice to an
26 authorized user regarding the download or installation of software in order to deceive
27 the consumer.
- 28 (10) 'Internet' means the global information system that is logically linked together by
29 a globally unique address space based on the Internet Protocol or its subsequent
30 extensions; that is able to support communications using the Transmission Control
31 Protocol/Internet Protocol suite, its subsequent extensions, or other Internet Protocol
32 compatible protocols; and that provides, uses, or makes accessible, either publicly or
33 privately, high level services layered on the communications and related infrastructure
34 described in this paragraph.
- 35 (11) 'Person' means any individual, partnership, corporation, limited liability company,
36 or other organization, or any combination thereof.
- 37 (12) 'Personally identifiable information' means any of the following:

- 1 (A) A first name or first initial in combination with a last name;
 2 (B) Credit or debit card numbers or other financial account numbers;
 3 (C) A password or personal identification number required to access an identified
 4 financial account;
 5 (D) A social security number; or
 6 (E) Any of the following information in a form that personally identifies an authorized
 7 user:
 8 (i) Account balances;
 9 (ii) Overdraft history;
 10 (iii) Payment history;
 11 (iv) A history of websites visited;
 12 (v) A home address;
 13 (vi) A work address; or
 14 (vii) A record of a purchase or purchases.

15 16-9-152.

- 16 (a) It shall be illegal for a person or entity that is not an authorized user, as defined in Code
 17 Section 16-9-151, of a computer in this state to knowingly, willfully, or with conscious
 18 indifference or disregard cause computer software to be copied onto such computer and use
 19 the software to do any of the following:
 20 (1) Modify, through intentionally deceptive means, any of the following settings related
 21 to the computer's access to, or use of, the Internet:
 22 (A) The page that appears when an authorized user launches an Internet browser or
 23 similar software program used to access and navigate the Internet;
 24 (B) The default provider or web proxy the authorized user uses to access or search the
 25 Internet; or
 26 (C) The authorized user's list of bookmarks used to access web pages;
 27 (2) Collect, through intentionally deceptive means, personally identifiable information
 28 that meets any of the following criteria:
 29 (A) It is collected through the use of a keystroke-logging function that records all
 30 keystrokes made by an authorized user who uses the computer and transfers that
 31 information from the computer to another person;
 32 (B) It includes all or substantially all of the websites visited by an authorized user,
 33 other than websites of the provider of the software, if the computer software was
 34 installed in a manner designed to conceal from all authorized users of the computer the
 35 fact that the software is being installed; or

1 (C) It is a data element described in subparagraph (B), (C), or (D) of paragraph (12)
2 of Code Section 16-9-151, or in division (i) or (ii) of subparagraph (E) of paragraph
3 (12) of Code Section 16-9-151, that is extracted from the consumer's or business
4 entity's computer hard drive for a purpose wholly unrelated to any of the purposes of
5 the software or service described to an authorized user;

6 (3) Prevent, without the authorization of an authorized user, through intentionally
7 deceptive means, an authorized user's reasonable efforts to block the installation of, or
8 to disable, software, by causing software that the authorized user has properly removed
9 or disabled to automatically reinstall or reactivate on the computer without the
10 authorization of an authorized user;

11 (4) Intentionally misrepresent that software will be uninstalled or disabled by an
12 authorized user's action, with knowledge that the software will not be so uninstalled or
13 disabled; or

14 (5) Through intentionally deceptive means, remove, disable, or render inoperative
15 security, antispyware, or antivirus software installed on the computer.

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

25 16-9-153.

26 (a) It shall be illegal for a person or entity that is not an authorized user, as defined in Code
27 Section 16-9-151, of a computer in this state to knowingly, willfully, or with conscious
28 indifference or disregard cause computer software to be copied onto such computer and use
29 the software to do any of the following:

30 (1) Take control of the consumer's or business entity's computer by doing any of the
31 following:

32 (A) Transmitting or relaying commercial electronic mail or a computer virus from the
33 consumer's or business entity's computer, where the transmission or relaying is
34 initiated by a person other than the authorized user and without the authorization of an
35 authorized user;

1 (B) Accessing or using the consumer's or business entity's modem or Internet service
2 for the purpose of causing damage to the consumer's or business entity's computer or
3 of causing an authorized user or a third party affected by such conduct to incur financial
4 charges for a service that is not authorized by an authorized user;

5 (C) Using the consumer's or business entity's computer as part of an activity
6 performed by a group of computers for the purpose of causing damage to another
7 computer, including, but not limited to, launching a denial of service attack; or

8 (D) Opening multiple, sequential, stand-alone advertisements in the consumer's or
9 business entity's Internet browser without the authorization of an authorized user and
10 with knowledge that a reasonable computer user cannot close the advertisements
11 without turning off the computer or closing the consumer's or business entity's Internet
12 browser;

13 (2) Modify any of the following settings related to the computer's access to, or use of,
14 the Internet:

15 (A) An authorized user's security or other settings that protect information about the
16 authorized user for the purpose of stealing personal information of an authorized user;
17 or

18 (B) The security settings of the computer for the purpose of causing damage to one or
19 more computers; or

20 (3) Prevent, without the authorization of an authorized user, an authorized user's
21 reasonable efforts to block the installation of, or to disable, software, by doing any of the
22 following:

23 (A) Presenting the authorized user with an option to decline installation of software
24 with knowledge that, when the option is selected by the authorized user, the installation
25 nevertheless proceeds; or

26 (B) Falsely representing that software has been disabled.

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

1 16-9-154.

2 (a) It shall be illegal for a person or entity that is not an authorized user, as defined in Code
3 Section 16-9-151, of a computer in this state to do any of the following with regard to such
4 computer:

5 (1) Induce an authorized user to install a software component onto the computer by
6 intentionally misrepresenting that installing software is necessary for security or privacy
7 reasons or in order to open, view, or play a particular type of content; or

8 (2) Deceptively causing the copying and execution on the computer of a computer
9 software component with the intent of causing an authorized user to use the component
10 in a way that violates any other provision of this Code section.

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

20 16-9-155.

21 (a) Any person who violates the provisions of paragraph (2) of Code Section 16-9-152,
22 subparagraph (A), (B), or (C) of paragraph (1) of subsection (a) of Code Section 16-9-153,
23 or paragraph (2) of subsection (a) of Code Section 16-9-153 shall be guilty of a felony and,
24 upon conviction thereof, shall be sentenced to imprisonment for not less than one nor more
25 than ten years or a fine of not more than \$3 million, or both.

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

28 (1) A civil penalty of up to \$100.00 per violation of this article, or up to \$100,000.00 for
29 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 (c) In the case of a violation of subparagraph (B) of paragraph (1) of subsection (a) of
33 Code Section 16-9-153 that causes a telecommunications carrier to incur costs for the
34 origination, transport, or termination of a call triggered using the modem of a customer of
35 such telecommunications carrier as a result of such violation, the telecommunications
36 carrier may bring a civil action against the violator to recover any or all of the following:

1 (1) The charges such carrier is obligated to pay to another carrier or to an information
2 service provider as a result of the violation, including, but not limited to, charges for the
3 origination, transport or termination of the call;

4 (2) Costs of handling customer inquiries or complaints with respect to amounts billed for
5 such calls;

6 (3) Costs and reasonable attorney's fees; and

7 (4) An order to enjoin the violation.

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

12 (1)(A) Statutory damages of not more than \$100.00 per violation of this article, or up
13 to \$1 million for a pattern or practice of such violations;

14 (2) Costs and reasonable attorney's fees; and

15 (3) An order to enjoin the violation.

16 16-9-156.

17 (a) For the purposes of this Code section, the term 'employer' includes a business entity's
18 officers, directors, parent corporation, subsidiaries, affiliates, and other corporate entities
19 under common ownership or control within a business enterprise. No employer may be
20 held criminally or civilly liable under this article as a result of any actions taken:

21 (1) With respect to computer equipment used by its employees, contractors,
22 subcontractors, agents, leased employees, or other staff which the employer owns, leases,
23 or otherwise makes available or allows to be connected to the employer's network or
24 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 (b) No person shall be held criminally or civilly liable under this article when its protected
29 computers have been used by unauthorized users to violate this article or other laws
30 without such person's knowledge, consent, or approval.

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

1 16-9-157.

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

7 **SECTION 2.**

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

10 **SECTION 3.**

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