Computer Security

This Act requires notices prior to certain software or programs being loaded onto certain computers and requires certain functions be available in certain software. The Act seems targeted toward prohibiting "hijacking" computers by which malicious software loads onto a user's personal computer and forces the user's browser to go to a specific Web site. The Act also seems to address a practice whereby malicious software continually reloads on a personal computer despite a user's attempts to delete or disable such software.

Submitted as:
Georgia
SB 127 (Enrolled version)
Status: Enacted into law in 2005.

Suggested State Legislation

Section 1. [*Short Title*.] This Act may be cited as "The Computer Security Act."

Section 2. [*Definitions*.] As used in this Act:

(1) "Computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device.

(2) "Disable" means, with respect to an information collection program, to permanently prevent such program from executing any of the functions described in paragraph (3) of this Act that such program is otherwise capable of executing by removing, deleting, or disabling the program unless the owner of a protected computer takes a subsequent affirmative action to enable the execution of such functions.

(3) "Information collection program" means computer software that:

(A) Collects personally identifiable information and sends such information to a person other than the owner or authorized user of the computer or uses such information to deliver advertising to or display advertising on the computer; or

(B) Collects information regarding the web pages accessed using the computer and uses such information to deliver advertising to or display advertising on the computer.

(4) "Internet" means collectively the myriad of 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.

(5) "'Personally identifiable information" means the following information, to the extent only that such information allows a living individual to be identified from that information:

(A) First and last name of an individual;

(B) A home or other physical address of an individual, including street name, name of a city or town, and ZIP Code;

(C) An electronic mail address;

(D) A telephone number;

(E) A social security number, tax identification number, passport number, driver's license number, or any other government issued identification number;

(F) A credit card number;

(G) Any access code, password, or account number, other than an access code or password transmitted by an owner or authorized user of a protected computer to the intended recipient to register for, or log onto, a webpage or other Internet service or a network connection or service of a subscriber that is protected by an access code or password; and

(H) Date of birth, birth certificate number, or place of birth of an individual, except in the case of a date of birth transmitted or collected for the purpose of compliance with the law.

(6) "Protected computer" means a computer which, at the time of an alleged violation of this Act involving that computer, is located within the geographic boundaries of this state.

(7) "Web page" means a location, with respect to the World Wide Web, that has a single uniform resource locator or another single location with respect to the Internet.

Section 3. [*Unlawful Deceptive Acts and Practices of a Protected Computer.*]

(1) It shall be an unlawful deceptive act or practice for any person who is not the owner or authorized user of a protected computer to engage in any of the following acts or practices with respect to a protected computer:

(A) Taking control of the computer by:

(i) Using such computer to send unsolicited information or material from the protected computer to others;

(ii) Diverting the Internet browser of the computer, or similar program of the computer used to access and navigate the Internet:

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

(b) Away from the site the user intended to view, to one or more other web pages, such that the user is prevented from viewing the content at the intended webpage, unless such diverting is otherwise authorized;

(iii) Accessing or using the modem or Internet connection or service for the computer and thereby causing damage to the computer or causing the owner or authorized user to incur unauthorized financial charges;

(iv) Using the computer as part of an activity performed by a group of computers that causes damage to another computer; or

(v) Delivering advertisements that a user of the computer cannot close without turning off the computer or closing all sessions of the Internet browser for the computer;

(vi) Modifying settings related to use of the computer or to the computer's access to or use of the Internet by altering:

(a) The webpage that appears when the owner or authorized user launches an Internet browser or similar program used to access and navigate the Internet;

(b) The default provider used to access or search the Internet, or other existing Internet connections settings;

(c) A list of bookmarks used by the computer to access web pages;

(d) Security or other settings of the computer that protect information about the owner or authorized user for the purposes of causing damage or harm to the computer or owner or user;

(vii) Collecting personally identifiable information through the use of a keystroke logging function;

(viii) Inducing the owner or authorized user to install a computer software component onto the computer, or preventing reasonable efforts to block the installation or execution of, or to disable, a computer software component by:

(a) Presenting the owner or authorized user with an option to decline installation of a software component such that, when the option is selected by the owner or authorized user, the installation nevertheless proceeds; or

(b) Causing a computer software component that the owner or authorized user has properly removed or disabled to reinstall or reactivate automatically on the computer;

(ix) Misrepresenting that installing a separate software component or providing log-in and password information is necessary for security or privacy reasons, or that installing a separate software component is necessary to open, view, or play a particular type of content;

(x) Inducing the owner or authorized user to install or execute computer software by misrepresenting the identity or authority of the person or entity providing the computer software to the owner or user;

(xi) Inducing the owner or authorized user to provide personally identifiable, password, or account information to another person:

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

(b) Without the authority of the intended recipient of the information;

(xii) Removing, disabling, or rendering inoperative a security, anti-spyware, or anti-virus technology installed on the computer; or

(xiii) Installing or executing on the computer one or more additional computer software components with the intent of causing a person to use such components in a way that violates any other provision of this Act.

(2) Except as otherwise provided in this Act, it shall be unlawful for any person:

(A) To transmit to a protected computer, which is not owned by such person and for which such person is not an authorized user, any information collection program, unless:

(i) Such information collection program provides notice in accordance with this Act before execution of any of the information collection functions of the program; and

(ii) Such information collection program includes the functions required under this Act; or

(B) To execute any information collection program installed on such a protected computer unless:

(i) Before execution of any of the information collection functions of the program, the owner or an authorized user of the protected computer has consented to such execution pursuant to notice in accordance with this Act; and

(ii) Such information collection program includes the functions required under this Act.

(iii) Notice in accordance with this Act with respect to an information collection program is clear and conspicuous notice in plain language that meets all of the following requirements:

(a) The notice clearly distinguishes such notice from any other information visually presented contemporaneously on the protected computer;

(b) The notice contains one of the following statements, as applicable, or a substantially similar statement:

(I) "This program will collect and transmit information about you. Do you accept?";

(II) "This program will collect information about web pages you access and will use that information to display advertising on your computer. Do you accept?"; or

(III) "This program will collect and transmit information about you and your computer use and will collect information about web pages you access and use that information to display advertising on your computer. Do you accept?";

(c) The notice provides for the user:

(I) To grant or deny consent by selecting an option to grant or deny such consent; and

(II) To abandon or cancel the transmission or execution without granting or denying such consent;

(d) The notice provides an option for the user to select to display on the computer, before granting or denying consent using the option required under this Act, a clear description of:

(I) The types of information to be collected and sent, if any, by the information collection program;

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

(III) In the case of an information collection program that first executes any of the information collection functions of the program together with the first execution of other computer software, the identity of any such software that is an information collection program; and

(e) The notice provides for concurrent display of the information required this Act and the option required under this Act until the user:

(I) Grants or denies consent using the option required under this Act;

(II) Abandons or cancels the transmission or execution under this Act; or

(III) Selects the option required under this Act.

(3) In the case in which multiple information collection programs are provided to the protected computer together, or as part of a suite of functionally related software, the notice requirements of this Act may be met by providing, before execution of any of the information collection functions of the programs, clear and conspicuous notice in plain language by means of a single notice that applies to all such information collection programs, except that such notice shall provide the option with respect to each such information collection program.

(4) If an owner or authorized user has granted consent to execution of an information collection program pursuant to a notice in accordance with this Act:

(A) No subsequent such notice is required, except as provided in subparagraph (B) of this paragraph; and

(B) The person who transmitted the program shall provide another notice in accordance with this Act and obtain consent before such program may be used to collect or send information of a type or for a purpose that is materially different from, and outside the scope of, the type or purpose set forth in the initial or any previous notice.

(5) The functions required under this Act to be included in an information collection program that executes any information collection functions with respect to a protected computer are as follows:

(A) Disabling function. With respect to any information collection program, a function of the program that allows a user of the program to remove the program or disable operation of the program with respect to such protected computer by a function that:

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

(ii) Can be performed without undue effort or knowledge by the user of the protected computer; and

(B) Identity function. With respect only to an information collection program, a function of the program that provides that each display of an advertisement directed or displayed using such information when the owner or authorized user is accessing a webpage or online location other than that of the provider of the software is accompanied by the name of the information collection program, a logogram or trademark used for the exclusive purpose of identifying the program, or a statement or other information sufficient to clearly identify the program.

(6) A telecommunications carrier, a provider of information service or interactive computer service, a cable operator, or a provider of transmission capability shall not be liable, criminally or civilly, under this Act to the extent that the carrier, operator, or provider:

(A) Transmits, routes, hosts, stores, or provides connections for an information collection program through a system or network controlled or operated by or for the carrier, operator, or provider; or

(B) Provides an information location tool, such as a directory, index, reference, pointer, or hypertext link, through which the owner or user of a protected computer locates an information collection program.

Section 4. [*Exceptions*.]

(1) This Act shall not apply to:

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

(B) The transmission or execution of an information collection program in compliance with a law enforcement, investigatory, national security, or regulatory agency or department of the United States or any state in response to a request or demand made under authority granted to that agency or department, including a warrant issued under the Federal Rules of Criminal Procedure, an equivalent state warrant, a court order, or other lawful process.

(C) Any monitoring of or interaction with a subscriber's Internet or other network connection or service, or a protected computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service, to the extent that such monitoring or interaction is for network or computer security purposes, diagnostics, technical support, or repair, or for the detection or prevention of fraudulent activities; or

(D) A discrete interaction with a protected computer by a provider of computer software solely to determine whether the user of the computer is authorized to use such software that occurs upon

(i) Initialization of the software; or

(ii) An affirmative request by the owner or authorized user for an update of, addition to, or technical service for the software.

(2) No provider of computer software or of interactive computer service may be held liable, criminally or civilly, under this Act on account of any action voluntarily taken, or service provided, in good faith to remove or disable a program used to violate this Act that is installed on a computer of a customer of such provider, if such provider notifies the customer and obtains the consent of the customer before undertaking such action or providing such service.

(3) A manufacturer or retailer of computer equipment shall not be liable under this Act, criminally or civilly, to the extent that the manufacturer or retailer is providing third-party branded software that is installed on the equipment the manufacturer or retailer is manufacturing or selling.

(4) For the purposes of this Act, the term "employer" includes a business's officers, directors, parent corporation, subsidiaries, affiliates, and other corporate entities under common ownership or control within an enterprise.

(5) No employer may be held liable criminally or civilly under this Act on account of any actions taken:

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

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

(6) No person shall be liable criminally or civilly under this Act when its protected computers have been used by unauthorized people to violate this Act or other laws without such person's knowledge, consent, or approval.

(7) No civil cause of action shall lie against any foreign or business in this state or its officers, employees, agents, or other people for providing computer-related records, information, facilities, or assistance to further the investigation of a criminal offense enumerated in [insert citation] to a law enforcement unit as [insert citation] or a prosecutorial office of this state when said computer-related records, information, facilities, or assistance is provided pursuant to a subpoena, search warrant, order to produce.

(8) Any business located within this state that provides electronic communication services or remote computing services as defined by [insert citation], when served with a search warrant, subpoena, notice to produce, notice of deposition, or order to disclose properly issued by another state to produce records related to investigation or trial of a criminal offense that would reveal the identity of their customers using those services, data stored by, or on behalf of, their customer, their 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 requested records as if that search warrant, subpoena, notice, or order had been issued by a state court, provided that such business has the right to object that such compliance is unduly burdensome or oppressive.

Section 5. [*Penalties*.]

(1) Any person who violates this Act shall be guilty of a [felony] and, upon conviction thereof, shall be sentenced to imprisonment for [not less than one nor more than ten years] or a fine of not more than [$3 million], or both.

(2) Any person who suffers personal, property, or economic damages by reason of a violation of this Act may initiate a civil action for and recover the greater of:

(A) [Five thousand dollars} plus expenses of litigation and reasonable attorney's fees;

(B) Liquidated damages of [$1,000] for each violation of up to a limit of [$2 million] per incident, plus expenses of litigation and reasonable attorney's fees; or

(C) Actual damages, plus expenses of litigation and reasonable attorney's fees.

Section 6. [*Severability*.] [Insert severability clause.]

Section 7. [*Repealer*.] [Insert repealer clause.]

Section 8. [*Effective Date.*] [Insert effective date.]