STATE OF NEW YORK

4444

2019-2020 Regular Sessions

IN SENATE

March 11, 2019

Introduced by Sen. PARKER -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology

AN ACT to amend the general business law, in relation to establishing "the computer security act"

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. Section 150 of the general business law is renumbered section 154.

§ 2. The general business law is amended by adding a new article 9-D to read as follows:

ARTICLE 9-D

THE COMPUTER SECURITY ACT

§ 150. Short title. This act shall be known and may be cited as "the computer security act."

§ 151. Definitions. For purposes of this article, the following terms shall have the following meanings:

1. "Advertisement" means a communication, the primary purpose of which is the commercial promotion of a commercial product or service, including content on an internet website operated for a commercial purpose.

2. "Authorized user," with respect to a computer, means a person who owns or is authorized by the owner or lessee to use the computer.

3. "Cause to be copied" means to distribute or transfer computer software or any component thereof. Such term shall not include providing:

a. Transmission, routing, provision of intermediate temporary storage, or caching of software;

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD10389-01-9

b. A storage medium, such as a compact disk, website, or computer server, through which the software was distributed by a third party; or

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

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

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

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

7. "Damage" means any significant impairment to the integrity or availability of data, software, a system, or information.

8. "Execute," when used with respect to computer software, means the performance of the functions or the carrying out of the instructions of the computer software.

9. "Intentionally deceptive" means any of the following:

a. By means of an intentionally and materially false or fraudulent statement;

b. By means of a statement or description that intentionally omits or misrepresents material information in order to deceive the consumer; or

c. By means of an intentional and material failure to provide any notice to an authorized user regarding the download or installation of software in order to deceive the consumer.

10. "Internet" means the global information system that is logically linked together by a globally unique address space based on the internet protocol or its subsequent extensions; that is able to support communications using the transmission control protocol/internet protocol suite, its subsequent extensions, or other internet protocol compatible protocols; and that provides, uses, or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described in this subdivision.

11. "Person" means any individual, partnership, corporation, limited liability company, or other organization, or any combination thereof.

12. "Personally identifiable information" means any of the following:

a. A first name or first initial in combination with a last name;

b. Credit or debit card numbers or other financial account numbers;

c. A password or personal identification number required to access an identified financial account;

d. A Social Security number; or

e. Any of the following information in a form that personally identifies an authorized user:

(1) Account balances;

(2) Overdraft history;

(3) Payment history;

(4) A history of websites visited;

(5) A home address;

(6) A work address; or

(7) A record of a purchase or purchases.

§ 152. Unlawful acts involving computer software. 1. It shall be illegal for a person or entity that is not an authorized user, as defined in section one hundred fifty-one of this article, of a computer in this state to knowingly, willfully, or with conscious indifference or disregard cause computer software to be copied onto such computer and use the software to do any of the following:

a. Modify, through intentionally deceptive means, any of the following settings related to the computer's access to, or use of, the internet:

(1) The page that appears when an authorized user launches an internet browser or similar software program used to access and navigate the internet;

(2) The default provider or web proxy the authorized user uses to access or search the internet; or

(3) The authorized user's list of bookmarks used to access web pages;

b. Collect, through intentionally deceptive means, personally identifiable information that meets any of the following criteria:

(1) It is collected through the use of a keystroke-logging function that records all keystrokes made by an authorized user who uses the computer and transfers that information from the computer to another person;

(2) It includes all or substantially all of the websites visited by an authorized user, other than websites of the provider of the software, if the computer software was installed in a manner designed to conceal from all authorized users of the computer the fact that the software is being installed; or

(3) It is a data element described in paragraph b, c, or d of subdivision twelve of section one hundred fifty-one of this article, or in subparagraph one or two of paragraph e of subdivision twelve of section one hundred fifty-one of this article, that is extracted from the consumer's or business entity's computer hard drive for a purpose wholly unrelated to any of the purposes of the software or service described to an authorized user;

c. Prevent, without the authorization of an authorized user, through intentionally deceptive means, an authorized user's reasonable efforts to block the installation of, or to disable, software, by causing software that the authorized user has properly removed or disabled to automatically reinstall or reactivate on the computer without the authorization of an authorized user;

d. Intentionally misrepresent that software will be uninstalled or disabled by an authorized user's action, with knowledge that the software will not be so uninstalled or disabled; or

e. Through intentionally deceptive means, remove, disable, or render inoperative security, antispyware, or antivirus software installed on the computer.

2. It shall be illegal for a person or entity that is not an authorized user, as defined in section one hundred fifty-one of this article, of a computer in this state to knowingly, willfully, or with conscious indifference or disregard cause computer software to be copied onto such computer and use the software to do any of the following:

a. Take control of the consumer's or business entity's computer by doing any of the following:

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

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

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

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

b. Modify any of the following settings related to the computer's access to, or use of, the internet:

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

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

c. Prevent, without the authorization of an authorized user, an authorized user's reasonable efforts to block the installation of, or to disable, software, by doing any of the following:

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

(2) Falsely representing the software has been disabled.

3. It shall be illegal for a person or entity that is not an authorized user, as defined in section one hundred fifty-one of this article, of a computer in this state to do any of the following with regard to such computer:

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

b. Deceptively causing the copying and execution on the computer of a computer software component with the intent of causing an authorized user to use the component in a way that violates any other provision of this subdivision.

4. Nothing in this section shall apply to any monitoring of, or interaction with, a user'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 for network or computer security purposes, diagnostics, technical support, repair, network management, network maintenance, authorized updates of software or system firmware, authorized remote system management, or detection or prevention of the unauthorized use of or fraudulent or other illegal activities in connection with a network, service, or computer software, including scanning for and removing software proscribed under this article.

§ 153. Penalties. 1. Any person who violates the provisions of paragraph b of subdivision one of section one hundred fifty-two of this article, subparagraph one, two, or three of paragraph a of subdivision two of section one hundred fifty-two of this article or paragraph b of

subdivision two of section one hundred fifty-two of this article 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 three million dollars, or both.

2. The attorney general may bring a civil action against any person violating the provisions of this article to the penalties for the violation and may recover any or all of the following:

a. A civil penalty of up to one hundred dollars per violation of this article, or up to one hundred thousand dollars for a pattern or practice of such violations;

b. Costs and reasonable attorney's fees; and

c. An order to enjoin the violation.

3. In the case of a violation of subparagraph two of paragraph a of subdivision two of section one hundred fifty-two of this article that causes a telecommunications carrier to incur costs for the origination, transport, or termination of a call triggered using the modem of a customer of such telecommunications carrier as a result of such violation, the telecommunications carrier may bring a civil action against the violator to recover any or all of the following:

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

b. Costs of handling customer inquiries or complaints with respect to amounts billed for such calls;

c. Costs and reasonable attorney's fees; and

d. An order to enjoin the violation.

4. An internet service provider or software company that expends resources in good faith assisting consumers or business entities harmed by a violation of this article, or a trademark owner whose mark is used to deceive consumers or business entities in violation of this article, may enforce the violation and may recover any or all of the following:

a. Statutory damages of not more than one hundred dollars per violation of this article, or up to one million dollars for a pattern or practice of such violations;

b. Costs and reasonable attorney's fees; and

c. An order to enjoin the violation.

§ 153-a. Immunity from liability for violations. 1. For the purposes of this section, the term "employer" includes a business entity's officers, directors, parent corporation, subsidiaries, affiliates, and other corporate entities under common ownership or control within a business enterprise. No employer may be held criminally or civilly liable under this article as a result of any actions taken:

a. With respect to computer equipment used by its employees, contractors, subcontractors, agents, leased employees, or other staff which the employer owns, leases, or otherwise makes available or 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.

2. No person shall be held criminally or civilly liable under this article when its protected computers have been used by unauthorized users to violate this article or other laws without such person's knowledge, consent, or approval.

3. A manufacturer or retailer of computer equipment shall not be liable under this section, criminally or civilly, to the extent that the

manufacturer or retailer is providing third party branded software that is installed on the computer equipment that the manufacturer or retailer is manufacturing or selling.

§ 153-b. Preempting other jurisdictional actions about spyware. The legislature finds that this article is a matter of state-wide concern. This article supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by any county, municipality, consolidated government, or other local governmental agency regarding spyware and notices to consumers from computer software providers regarding information collection.

§ 3. This act shall take effect on the first of November next succeeding the date on which it shall have become a law.