

STATE OF NEW YORK

8641

2017-2018 Regular Sessions

IN ASSEMBLY

September 1, 2017

Introduced by M. of A. KAVANAGH -- read once and referred to the Committee on Economic Development

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:

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

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

ARTICLE 9-D

THE COMPUTER SECURITY ACT

7 Section 150. Short title.

8 151. Definitions.

9 152. Unlawful acts involving computer software.

10 153. Penalties.

11 153-a. Immunity from liability for violations.

12 153-b. Preempting other jurisdictional actions about spyware.

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

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

17 1. "Advertisement" means a communication, the primary purpose of which
18 is the commercial promotion of a commercial product or service, includ-
19 ing content on an internet website operated for a commercial purpose.

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

22 3. "Cause to be copied" means to distribute or transfer computer soft-
23 ware or any component thereof. Such term shall not include providing:

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

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

LBD01923-01-7

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

3 c. An information location tool, such as a directory, index, refer-
4 ence, pointer, or hypertext link, through which the user of the computer
5 located the software.

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

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

15 6. "Consumer" means an individual who resides in this state and who
16 uses the computer in question primarily for personal, family, or house-
17 hold purposes.

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

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

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

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

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

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

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

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

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

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

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

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

46 d. A Social Security number; or

47 e. Any of the following information in a form that personally identi-
48 fies an authorized user:

49 (1) Account balances;

50 (2) Overdraft history;

51 (3) Payment history;

52 (4) A history of websites visited;

53 (5) A home address;

54 (6) A work address; or

55 (7) A record of a purchase or purchases.

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

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

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

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

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

15 b. Collect, through intentionally deceptive means, personally iden-
16 tifiable information that meets any of the following criteria:

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

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

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

33 c. Prevent, without the authorization of an authorized user, through
34 intentionally deceptive means, an authorized user's reasonable efforts
35 to block the installation of, or to disable, software, by causing soft-
36 ware that the authorized user has properly removed or disabled to auto-
37 matically reinstall or reactivate on the computer without the authori-
38 zation of an authorized user;

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

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

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

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

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

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

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

10 (4) Opening multiple, sequential, stand-alone advertisements in the
11 consumer's or business entity's internet browser without the authori-
12 zation of an authorized user and with knowledge that a reasonable
13 computer user cannot close the advertisements without turning off the
14 computer or closing the consumer's or business entity's internet brow-
15 ser;

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

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

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

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

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

29 (2) Falsely representing the software has been disabled.

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

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

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

42 4. Nothing in this section shall apply to any monitoring of, or inter-
43 action with, a user's internet or other network connection or service,
44 or a protected computer, by a telecommunications carrier, cable opera-
45 tor, computer hardware or software provider, or provider of information
46 service or interactive computer service for network or computer security
47 purposes, diagnostics, technical support, repair, network management,
48 network maintenance, authorized updates of software or system firmware,
49 authorized remote system management, or detection or prevention of the
50 unauthorized use of or fraudulent or other illegal activities in
51 connection with a network, service, or computer software, including
52 scanning for and removing software proscribed under this article.

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

1 subdivision two of section one hundred fifty-two of this article shall
2 be guilty of a felony and, upon conviction thereof, shall be sentenced
3 to imprisonment for not less than one nor more than ten years or a fine
4 of not more than three million dollars, or both.

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

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

11 b. Costs and reasonable attorney's fees; and

12 c. An order to enjoin the violation.

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

20 a. The charges such carrier is obligated to pay to another carrier or
21 to an information service provider as a result of the violation, includ-
22 ing, but not limited to, charges for the origination, transport or
23 termination of the call;

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

26 c. Costs and reasonable attorney's fees; and

27 d. An order to enjoin the violation.

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

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

36 b. Costs and reasonable attorney's fees; and

37 c. An order to enjoin the violation.

38 § 153-a. Immunity from liability for violations. 1. For the purposes
39 of this section, the term "employer" includes a business entity's offi-
40 cers, directors, parent corporation, subsidiaries, affiliates, and other
41 corporate entities under common ownership or control within a business
42 enterprise. No employer may be held criminally or civilly liable under
43 this article as a result of any actions taken:

44 a. With respect to computer equipment used by its employees, contrac-
45 tors, subcontractors, agents, leased employees, or other staff which the
46 employer owns, leases, or otherwise makes available or allows to be
47 connected to the employer's network or other computer facilities; or

48 b. By employees, contractors, subcontractors, agents, leased employ-
49 ees, or other staff who misuse an employer's computer equipment for an
50 illegal purpose without the employer's knowledge, consent, or approval.

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

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

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

4 § 153-b. Preempting other jurisdictional actions about spyware. The
5 legislature finds that this article is a matter of state-wide concern.
6 This article supersedes and preempts all rules, regulations, codes,
7 ordinances, and other laws adopted by any county, municipality, consol-
8 idated government, or other local governmental agency regarding spyware
9 and notices to consumers from computer software providers regarding
10 information collection.

11 § 3. This act shall take effect on the first of November next succeed-
12 ing the date on which it shall have become a law.