

LEGISLATURE OF NEBRASKA
NINETY-NINTH LEGISLATURE
FIRST SESSION

LEGISLATIVE BILL 316

Introduced by Howard, 9

Read first time January 11, 2005

Committee: Judiciary

A BILL

- 1 FOR AN ACT relating to computers; to adopt the Consumer Protection
- 2 Against Computer Spyware Act.
- 3 Be it enacted by the people of the State of Nebraska,

1 Section 1. This act shall be known and may be cited as
2 the Consumer Protection Against Computer Spyware Act.

3 Sec. 2. For purposes of the Consumer Protection Against
4 Computer Spyware Act:

5 (1) Advertisement means a communication, the primary
6 purpose of which is the commercial promotion of a commercial
7 product or service, including content on an Internet site operated
8 for a commercial purpose;

9 (2) Authorized user, with respect to a computer, means a
10 person who owns or is authorized by the owner or lessee to use the
11 computer. Authorized user does not include a person that has
12 obtained authorization to use the computer solely through the use
13 of an end-user license agreement;

14 (3) Computer software means a sequence of instructions
15 written in any programming language that is executed on a computer;

16 (4) Computer virus means a computer program or other set
17 of instructions that is designed to degrade the performance of or
18 disable a computer or computer network and is designed to have the
19 ability to replicate itself on other computers or computer networks
20 without the authorization of the owners of those computers or
21 computer networks;

22 (5) Consumer means an individual who resides in this
23 state and who uses the computer in question primarily for personal,
24 family, or household purposes;

25 (6) Damage means any significant impairment to the
26 integrity or availability of data, computer software, a system, or
27 information;

28 (7) Execute, when used with respect to computer software,

1 means the performance of the functions or the carrying out of the
2 instructions of the computer software;

3 (8) Intentionally deceptive means any of the following:

4 (a) By means of an intentionally and materially false or
5 fraudulent statement;

6 (b) By means of a statement or description that
7 intentionally omits or misrepresents material information in order
8 to deceive the consumer; or

9 (c) By means of an intentional and material failure to
10 provide any notice to an authorized user regarding the download or
11 installation of computer software in order to deceive the consumer;

12 (9) Internet means the global information system that is
13 logically linked together by a globally unique address space based
14 on the Internet protocol, or its subsequent extensions, and that is
15 able to support communications using the transmission control
16 protocol/Internet protocol suite, or its subsequent extensions, or
17 other Internet protocol compatible protocols, and that provides,
18 uses, or makes accessible, either publicly or privately, high-level
19 services layered on the communications and related infrastructure
20 described in this subdivision;

21 (10) Person means any individual, partnership,
22 corporation, limited liability company, or other organization; and

23 (11) Personally identifiable information means any of the
24 following:

25 (a) First name or first initial in combination with last
26 name;

27 (b) Credit or debit card numbers or other financial
28 account numbers;

1 (c) A password or personal identification number required
2 to access an identified financial account;

3 (d) Social security number;

4 (e) Any of the following information in a form that
5 personally identifies an authorized user:

6 (i) Account balances;

7 (ii) Overdraft history;

8 (iii) Payment history;

9 (iv) History of web sites visited;

10 (v) Home address;

11 (vi) Work address; or

12 (vii) Record of a purchase.

13 Sec. 3. A person that is not an authorized user shall
14 not, with actual knowledge, with conscious avoidance of actual
15 knowledge, or willfully, cause computer software to be copied onto
16 the computer of a consumer in this state and use the computer
17 software to do any of the following:

18 (1) Modify, through intentionally deceptive means, any of
19 the following settings related to the computer's access to, or use
20 of, the Internet:

21 (a) The page that appears when an authorized user
22 launches an Internet browser or similar software program used to
23 access and navigate the Internet;

24 (b) The default provider or web proxy the authorized user
25 uses to access or search the Internet; or

26 (c) The authorized user's list of bookmarks used to
27 access web sites;

28 (2) Collect, through intentionally deceptive means,

1 personally identifiable information that meets any of the following
2 criteria:

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

7 (b) It includes all or substantially all of the web sites
8 visited by an authorized user, other than web sites of the provider
9 of the software, if the computer software was installed in a manner
10 designed to conceal from all authorized users of the computer the
11 fact that the software is being installed;

12 (c) It is a data element described in subdivision
13 (11) (b), (c), (d), (e) (i), or (e) (ii) of section 2 of this act that
14 is extracted from the consumer's computer hard drive for a purpose
15 wholly unrelated to any of the purposes of the computer software or
16 service described to an authorized user;

17 (3) Prevent, without the authorization of an authorized
18 user, through intentionally deceptive means, an authorized user's
19 reasonable efforts to block the installation of, or to disable,
20 computer software, by causing computer software that the authorized
21 user has properly removed or disabled to automatically reinstall or
22 reactivate on the computer without the authorization of an
23 authorized user;

24 (4) Intentionally misrepresent that computer software
25 will be uninstalled or disabled by an authorized user's action,
26 with knowledge that the computer software will not be so
27 uninstalled or disabled; or

28 (5) Through intentionally deceptive means, remove,

1 disable, or render inoperative security, antispymware, or antivirus
2 computer software installed on the computer.

3 Sec. 4. A person or entity that is not an authorized
4 user shall not, with actual knowledge, with conscious avoidance of
5 actual knowledge, or willfully, cause computer software to be
6 copied onto the computer of a consumer in this state and use the
7 computer software to do any of the following:

8 (1) Take control of the consumer's computer by doing any
9 of the following:

10 (a) Transmitting or relaying commercial electronic mail
11 or a computer virus from the consumer's computer if the
12 transmission or relaying is initiated by a person other than the
13 authorized user and without the authorization of an authorized
14 user;

15 (b) Accessing or using the consumer's modem or Internet
16 service for the purpose of causing damage to the consumer's
17 computer or of causing an authorized user to incur financial
18 charges for a service that is not authorized by an authorized user;

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

23 (d) Opening multiple, sequential, stand-alone
24 advertisements in the consumer's Internet browser without the
25 authorization of an authorized user and with knowledge that a
26 reasonable computer user cannot close the advertisements without
27 turning off the computer or closing the consumer's Internet
28 browser; or

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

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

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

8 (3) Prevent, without the authorization of an authorized
9 user, an authorized user's reasonable efforts to block the
10 installation of, or to disable, computer software, by doing any of
11 the following:

12 (a) Presenting the authorized user with an option to
13 decline installation of computer software with knowledge that, when
14 the option is selected by the authorized user, the installation
15 nevertheless proceeds; or

16 (b) Falsely representing that computer software has been
17 disabled.

18 This section does not apply to any monitoring of, or
19 interaction with, a subscriber's Internet or other network
20 connection or service, or a protected computer, by a
21 telecommunications carrier, cable operator, computer hardware or
22 software provider, or provider of information service or
23 interactive computer service for computer network or computer
24 security purposes, diagnostics, technical support, repair,
25 authorized updates of computer software or system firmware,
26 authorized remote system management, or detection or prevention of
27 the unauthorized use of or fraudulent or other illegal activities
28 in connection with a network, service, or computer software,

1 including scanning for and removing computer software proscribed
2 under the Consumer Protection Against Computer Spyware Act.

3 Sec. 5. A person who is not an authorized user shall not
4 do any of the following with regard to the computer of a consumer
5 in this state:

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

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

15 This section does not apply to any monitoring of, or
16 interaction with, a subscriber's Internet or other network
17 connection or service, or a protected computer, by a
18 telecommunications carrier, cable operator, computer hardware or
19 software provider, or provider of information service or
20 interactive computer service for computer network or computer
21 security purposes, diagnostics, technical support, repair,
22 authorized updates of computer software or system firmware,
23 authorized remote system management, or detection or prevention of
24 the unauthorized use of or fraudulent or other illegal activities
25 in connection with a network, service, or computer software,
26 including scanning for and removing computer software proscribed
27 under the Consumer Protection Against Computer Spyware Act.

28 Sec. 6. (1) The Task Force on Computer Technology and

1 Privacy is created. The task force shall:

2 (a) Examine the problems associated with computer privacy
3 and unauthorized access;

4 (b) Make recommendations on enforcement of the Consumer
5 Protection Against Computer Spyware Act and enforcement cooperation
6 with other states;

7 (c) Make recommendations for implementation of the act;
8 and

9 (d) Make recommendations for additional necessary
10 legislation concerning computer privacy and unauthorized computer
11 access.

12 The task force shall make any recommendations in a report
13 to the Governor and the Legislature by August 1, 2006.

14 (2) The task force shall have seven members appointed by
15 the Governor. The members shall have expertise in computer
16 software development, computer technology, the Internet, web site
17 development, or business use of computer and web technologies.
18 Members shall be reimbursed for their actual and necessary expenses
19 as provided in sections 81-1174 to 81-1177.

20 (3) For administrative purposes the task force shall be
21 located in the Public Service Commission. The commission shall
22 provide administrative support to the task force.

23 (4) The task force and this section terminate on August
24 1, 2006.

25 Sec. 7. Any person who violates any provision of the
26 Consumer Protection Against Computer Spyware Act is guilty of a
27 Class I misdemeanor for each violation.