

FIRST REGULAR SESSION

HOUSE BILL NO. 902

93RD GENERAL ASSEMBLY

INTRODUCED BY REPRESENTATIVES PRATT (Sponsor) AND PEARCE (Co-sponsor).

Read 1st time March 31, 2005 and copies ordered printed.

STEPHEN S. DAVIS, Chief Clerk

1318L.011

AN ACT

To amend chapter 407, RSMo, by adding thereto six new sections relating to computer spyware.

Be it enacted by the General Assembly of the state of Missouri, as follows:

Section A. Chapter 407, RSMo, is amended by adding thereto six new sections, to be
2 known as sections 407.1380, 407.1383, 407.1386, 407.1389, 407.1392, and 407.1395, to read
3 as follows:

**407.1380. 1. Sections 407.1380 to 407.1395 shall be known as and may be cited as
2 the "Consumer Protection Against Computer Spyware Act".**

**407.1383. For purposes of sections 407.1380 to 407.1395, the following terms shall
2 mean:**

3 (1) "Advertisement", a communication, the primary purpose of which is the
4 commercial promotion of a commercial product or service, including content on an
5 Internet web site operated for a commercial purpose;

6 (2) "Authorized user", with respect to a computer, a person who owns or is
7 authorized by the owner or lessee to use the computer. The term shall not include a person
8 or entity that has obtained authorization to use the computer solely through the use of an
9 end-user license agreement;

10 (3) "Computer software", a sequence of instructions written in any programming
11 language that is executed on a computer;

12 (4) "Computer virus", a computer program or other set of instructions that is
13 designed to degrade the performance of or disable a computer or computer network and
14 is designed to have the ability to replicate itself on other computers or computer networks

EXPLANATION — Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and is intended to be omitted from the law. Matter in **bold-face** type in the above bill is proposed language.

15 without the authorization of the owners of those computers or computer networks;

16 (5) "Consumer", an individual who resides in the state and who uses a computer
17 primarily for personal, family, or household purposes;

18 (6) "Damage", any significant impairment to the integrity or availability of data,
19 software, a system, or information;

20 (7) "Execute", when used with respect to computer software, the performance of
21 the functions or the carrying out of the instructions of the computer software;

22 (8) "Intentionally deceptive", any of the following:

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

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

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

29 (9) "Internet", the global information system that is logically linked together by a
30 globally unique address space based on the Internet protocol, or its subsequent extensions,
31 and that is able to support communications using the Transmission Control
32 Protocol/Internet Protocol suite, or its subsequent extensions, or other Internet
33 protocol-compatible protocols, and that provides, uses, or makes accessible, either publicly
34 or privately, high level services layered on the communications and related infrastructure
35 described in this subdivision;

36 (10) "Person", any individual, partnership, corporation, limited liability company,
37 or other organization, or any combination thereof;

38 (11) "Personally identifiable information", any of the following:

39 (a) A first name or first initial in combination with last name;

40 (b) Any credit or debit card numbers or other financial account numbers;

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

43 (d) A Social Security number;

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

46 a. Account balance;

47 b. Overdraft history;

48 c. Payment history;

49 d. History of web sites visited;

50 e. Home address;

51 f. Work address;

52 g. Record of a purchase or purchases.

2 **407.1386. A person or entity that is not an authorized user, as defined in section**
3 **407.1383 shall not, with actual knowledge, with conscious avoidance of actual knowledge,**
4 **or willfully, cause computer software to be copied onto the computer of a consumer in this**
5 **state and use the software to do any of the following:**

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

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

10 (b) **The default provider or web proxy the authorized user uses to access or search**
11 **the Internet;**

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

13 (2) **Collect, through intentionally deceptive means, personally identifiable**
14 **information that meets any of the following criteria:**

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

18 (b) **It includes all or substantially all of the web sites visited by an authorized user,**
19 **other than web sites of the provider of the software, if the computer software was installed**
20 **in a manner designed to conceal from all authorized users of the computer the fact that the**
21 **software is being installed;**

22 (c) **It is a data element described in paragraph (b), (c), or (d) of subdivision (11) of**
23 **section 407.1383, or in subparagraph a. or b. of paragraph (e) of subdivision (11) of section**
24 **407.1383, that is extracted from the consumer's computer hard drive for a purpose wholly**
25 **unrelated to any of the purposes of the software or service described to an authorized user;**

26 (3) **Prevent, without the authorization of an authorized user, through intentionally**
27 **deceptive means, an authorized user's reasonable efforts to block the installation of, or to**
28 **disable, software, by causing software that the authorized user has properly removed or**
29 **disabled to automatically reinstall or reactivate on the computer without the authorization**
30 **of an authorized user;**

31 (4) **Intentionally misrepresent that software will be uninstalled or disabled by an**
32 **authorized user's action, with knowledge that the software will not be so uninstalled or**
33 **disabled;**

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

407.1389. A person or entity that is not an authorized user, as defined in section 2 **407.1383**, shall not, with actual knowledge, with conscious avoidance of actual knowledge, 3 or willfully, cause computer software to be copied onto the computer of a consumer in this 4 state and use the software to do any of the following:

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

(a) Transmitting or relaying commercial electronic mail or a computer virus from 6 the consumer's computer, where the transmission or relaying is initiated by a person other 7 than the authorized user and without the authorization of an authorized user;

(b) Accessing or using the consumer's modem or Internet service for the purpose 9 of causing damage to the consumer's computer or of causing an authorized user to incur 10 financial charges for a service that is not authorized by an authorized user;

(c) Using the consumer's computer as part of an activity performed by a group of 12 computers for the purpose of causing damage to another computer, including, but not 13 limited to, launching a denial of service attack;

(d) Opening multiple, sequential, stand-alone advertisements in the consumer's 15 Internet browser without the authorization of an authorized user and with knowledge that 16 a reasonable computer user cannot close the advertisements without turning off the 17 computer or closing the consumer's Internet browser;

(2) Modify any of the following settings related to the computer's access to, or use 19 of, the Internet:

(a) An authorized user's security or other settings that protect information about 21 the authorized user for the purpose of stealing personal information of an authorized user;

(b) The security settings of the computer for the purpose of causing damage to one 23 or more computers;

(3) Prevent, without the authorization of an authorized user, an authorized user's 25 reasonable efforts to block the installation of, or to disable, software, by doing any of the 26 following:

(a) Presenting the authorized user with an option to decline installation of software 28 with knowledge that, when the option is selected by the authorized user, the installation 29 nevertheless proceeds;

(b) Falsely representing that software has been disabled;

(4) Nothing in this section shall apply to any monitoring of, or interaction with, a 32 subscriber's Internet or other network connection or service, or a protected computer, by 33 a telecommunications carrier, cable operator, computer hardware or software provider, 34 or provider of information service or interactive computer service for network or computer 35 security purposes, diagnostics, technical support, repair, authorized updates of software 36

37 or system firmware, authorized remote system management, or detection or prevention of
38 the unauthorized use of or fraudulent or other illegal activities in connection with a
39 network, service, or computer software, including scanning for and removing software
40 proscribed under this chapter.

2 **407.1392. 1.** A person or entity, who is not an authorized user, as defined in section
3 this state:

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

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

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

2 **407.1395.** It is the intent of the general assembly that sections 407.1380 to 407.1395
3 are a matter of statewide concern. This chapter supersedes and preempts all rules,
4 regulations, codes, ordinances, and other laws adopted by a city, county, city and county,
5 municipality, or local agency regarding spyware and notices to consumers from computer
software providers regarding information collection.