

**SUBSTITUTE FOR  
SENATE BILL NO. 151**

A bill to prohibit certain conduct relating to computer software, including spyware, and the unauthorized collection and use of information from computers; to prescribe the powers and duties of certain state agencies and officers; and to provide remedies.

**THE PEOPLE OF THE STATE OF MICHIGAN ENACT:**

1           Sec. 1. This act shall be known and may be cited as the  
2 "spyware control act".

3           Sec. 2. As used in this act:

4           (a) "Advertisement" means a communication, the primary purpose  
5 of which is the commercial promotion of a commercial product or  
6 service, including content on an internet website operated for a  
7 commercial purpose.

1 (b) "Authorized user" means the owner of the computer or a  
2 person who is authorized by the owner or lessee of the computer to  
3 use the computer.

4 (c) "Computer" means that term as defined in section 2 of 1979  
5 PA 53, MCL 752.792.

6 (d) "Computer software" means a sequence of instructions  
7 written in any programming language that is executed on a computer.  
8 Computer software does not include a cookie.

9 (e) "Computer virus" means a computer program or other set of  
10 instructions that is designed to damage, degrade the performance  
11 of, or disable a computer, computer data, or a computer network and  
12 to replicate itself on other computers or computer networks without  
13 the authorization of the owners of those computers or computer  
14 networks.

15 (f) "Cookie" means a nonexecutable text or data file that is  
16 used by, or placed on, a computer, computer program, computer  
17 system, or computer network, by an internet service provider,  
18 interactive computer service, or internet website to return  
19 information to that provider, service, or website, or to any device  
20 such as a web beacon to facilitate the use of the computer,  
21 computer program, computer system, or computer network by an  
22 authorized user.

23 (g) "Damage" means any significant impairment to the integrity  
24 or availability of data, software, a system, or information.

25 (h) "Deceptively" means by means of 1 or more of the  
26 following:

27 (i) An intentionally and materially false or fraudulent

1 pretense or statement.

2 (ii) A statement or description that omits or misrepresents  
3 material information in order to deceive an authorized user.

4 (iii) A material failure to provide any notice to an authorized  
5 user regarding the download or installation of software in order to  
6 deceive an authorized user.

7 (i) "Execute" means to perform the functions of or to carry  
8 out the instructions of computer software.

9 (j) "Internet" means that term as defined in 47 USC 230.

10 (k) "Person" means an individual, partnership, corporation,  
11 limited liability company, or other legal entity, or any  
12 combination of persons.

13 (l) "Personal identifying information" means that term as  
14 defined in section 3 of the identity theft protection act, 2004 PA  
15 452, MCL 445.63, or a name, number, or other information used as a  
16 password or access code.

17 Sec. 3. A person that is not an authorized user shall not,  
18 with actual knowledge, with conscious avoidance of actual  
19 knowledge, or willfully, cause computer software to be copied onto  
20 a computer in this state and use the computer software to do 1 or  
21 more of the following:

22 (a) Deceptively modify 1 or more of the following settings  
23 related to the computer's access to, or use of, the internet:

24 (i) The page that appears when an authorized user launches an  
25 internet browser or similar software program used to access and  
26 navigate the internet.

27 (ii) The default provider or web proxy an authorized user uses

1 to access or search the internet.

2 (iii) An authorized user's list of bookmarks used to access web  
3 pages.

4 (b) Deceptively collect personal identifying information that  
5 meets 1 or more of the following criteria:

6 (i) The information is collected through the use of a  
7 keystroke-logging function that records keystrokes made by an  
8 authorized user to transfer that information from the computer to  
9 another person.

10 (ii) If the computer software was installed in a manner  
11 designed to conceal the installation from authorized users of the  
12 computer, the information includes websites visited by an  
13 authorized user, other than websites of the provider of the  
14 software.

15 (iii) The information is extracted from the computer's hard  
16 drive for a purpose unrelated to any of the purposes of the  
17 computer software or service described to an authorized user.

18 (c) Deceptively prevent, without the authorization of an  
19 authorized user, an authorized user's reasonable efforts to disable  
20 or to block the reinstallation of software by causing software that  
21 the authorized user has properly removed or disabled to  
22 automatically reinstall or reactivate on the computer without the  
23 authorization of an authorized user.

24 (d) Misrepresent that software will be uninstalled or disabled  
25 by an authorized user's action, with knowledge that the software  
26 will not be uninstalled or disabled by the action.

27 (e) Deceptively remove, disable, or render inoperative

1 security, antispyware, or antivirus computer software installed on  
2 the computer.

3       Sec. 4. (1) A person that is not an authorized user shall not,  
4 with actual knowledge, with conscious avoidance of actual  
5 knowledge, or willfully, cause computer software to be copied onto  
6 a computer in this state and use the software to do 1 or more of  
7 the following:

8       (a) Take control of the computer by doing 1 or more of the  
9 following:

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

14       (ii) Accessing or using the modem or internet service of an  
15 authorized user for the purpose of causing damage to the computer  
16 or of causing an authorized user to incur financial charges for a  
17 service that is not authorized by an authorized user.

18       (iii) Using the computer as part of an activity performed by a  
19 group of computers for the purpose of causing damage to another  
20 computer, including, but not limited to, launching a denial of  
21 service attack.

22       (iv) Opening multiple, sequential, stand-alone advertisements  
23 in the authorized user's internet browser without the authorization  
24 of an authorized user and with knowledge that a reasonable computer  
25 user cannot close the advertisements without turning off the  
26 computer or closing the internet browser.

27       (b) Modify 1 or more of the following settings related to the

1 computer's access to, or use of, the internet:

2 (i) An authorized user's security or other settings that  
3 protect information about the authorized user, for the purpose of  
4 stealing personal identifying information of an authorized user.

5 (ii) The security settings of the computer, for the purpose of  
6 causing damage to 1 or more computers.

7 (c) Prevent, without the authorization of an authorized user,  
8 an authorized user's reasonable efforts to block the installation  
9 of, or to disable, software, by doing 1 or more of the following:

10 (i) Presenting the authorized user with an option to decline  
11 installation of software with knowledge that if the option is  
12 selected by the authorized user the installation nevertheless  
13 proceeds.

14 (ii) Falsely representing that software has been disabled.

15 (2) This section does not apply to monitoring of or  
16 interaction with an authorized user's internet or other network  
17 connection or service, or a computer by a telecommunications  
18 carrier, cable operator, computer hardware or software provider, or  
19 provider of information service or interactive computer service if  
20 the monitoring or interaction is for purposes of network or  
21 computer security, diagnostics, technical support, repair,  
22 authorized updates of software or system firmware, network  
23 management or maintenance, authorized remote system management, or  
24 detection or prevention of the unauthorized use of or fraudulent or  
25 other illegal activities in connection with a network, service, or  
26 computer software, including scanning for and removing software  
27 proscribed under this act.

1           Sec. 5. (1) A person who is not an authorized user shall not  
2 do 1 or more of the following to a computer in this state:

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

7           (b) Deceptively causing the copying and execution on the  
8 computer of a computer software component that causes the computer  
9 to use the component in a way that violates this section.

10           (2) This section does not apply to monitoring of or  
11 interaction with an authorized user's internet or other network  
12 connection or service or a computer by a telecommunications  
13 carrier, cable operator, computer hardware or software provider, or  
14 provider of information service or interactive computer service if  
15 the monitoring or interaction is for the purposes of network or  
16 computer security, diagnostics, technical support, repair,  
17 authorized updates of software or system firmware, network  
18 management or maintenance, authorized remote system management, or  
19 detection or prevention of the unauthorized use of or fraudulent or  
20 other illegal activities in connection with a network, service, or  
21 computer software, including scanning for and removing software  
22 proscribed under this act.

23           Sec. 6. (1) An action against a person for a violation of this  
24 act may be brought by the attorney general or by any of the  
25 following who is adversely affected by the violation:

26           (a) An authorized user.

27           (b) An internet website owner or registrant.

1 (c) A trademark or copyright owner.

2 (d) An authorized advertiser on an internet website.

3 (2) In an action under subsection (1), the person bringing the  
4 action may obtain 1 or both of the following:

5 (a) An injunction to prohibit further violations of this act.

6 (b) The greater of the following:

7 (i) Actual damages sustained by the person or, if the action is  
8 brought by the attorney general, by each person adversely affected  
9 by a violation that is a basis for the action.

10 (ii) Ten thousand dollars for each separate violation of this  
11 act.

12 (iii) If the defendant has engaged in a pattern and practice of  
13 violating this act, in the discretion of the court, up to 3 times  
14 whichever amount described in subparagraph (i) or (ii) is larger.

15 (3) In an action under subsection (1), a prevailing party is  
16 entitled to recover the actual costs of the action and reasonable  
17 attorney fees incurred.

18 (4) A single action or conduct that violates more than 1  
19 subdivision of sections 3 to 5 constitutes multiple violations of  
20 this act.

21 (5) The remedies provided by this section are in addition to  
22 any other remedies provided by law.

23 (6) A person shall not file a class action under this act.