SENATE BILL No. 145

January 31, 2007, Introduced by Senators BROWN, JELINEK, KAHN, RICHARDVILLE, BASHAM, BIRKHOLZ, CROPSEY and PAPPAGEORGE and referred to the Committee on Judiciary.

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:

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

Sec. 2. As used in this act:

(a) "Advertisement" means a communication, the primary purpose of which is the commercial promotion of a commercial product or

SENATE BILL No. 145

service, including content on an internet website operated for a commercial purpose.

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

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

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

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

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

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

(h) "Deceptively" means by means of 1 or more of the

following:

(*i*) An intentionally and materially false or fraudulent pretense or statement.

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

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

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

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

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

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

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

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

(*i*) The page that appears when an authorized user launches an internet browser or similar software program used to access and

navigate the internet.

(*ii*) The default provider or web proxy an authorized user uses to access or search the internet.

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

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

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

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

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

(c) Deceptively prevent, without the authorization of an authorized user, an authorized user's reasonable efforts to disable or to block the reinstallation of 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) Misrepresent that software will be uninstalled or disabled by an authorized user's action, with knowledge that the software

will not be uninstalled or disabled by the action.

(e) Deceptively remove, disable, or render inoperative security, antispyware, or antivirus computer software installed on the computer.

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

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

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

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

(*iii*) Using the 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.

(*iv*) Opening multiple, sequential, stand-alone advertisements in the authorized user'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 internet browser.

(b) Modify 1 or more of the following settings related to the computer's access to, or use of, the internet:

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

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

(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 1 or more of the following:

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

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

(2) This section does not apply to monitoring of or interaction with an authorized user's internet or other network connection or service, or a computer by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service if the monitoring or interaction is for purposes of network or computer security, diagnostics, technical support, repair, authorized updates of software or system firmware, network management or maintenance, 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 act.

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

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

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

(2) This section does not apply to monitoring of or interaction with an authorized user's internet or other network connection or service or a computer by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service if the monitoring or interaction is for the purposes of network or computer security, diagnostics, technical support, repair, authorized updates of software or system firmware, network management or maintenance, 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 act.

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

(a) An authorized user.

(b) An internet website owner or registrant.

(c) A trademark or copyright owner.

(d) An authorized advertiser on an internet website.

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

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

(b) The greater of the following:

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

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

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

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

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

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

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