Legislative Analysis

Mitchell Bean, Director
Phone: (517) 373-8080
http://www.house.mi.gov/hfa

SPYWARE

Senate Bill 53 (Substitute S-2)
Senate Bill 54 (Substitute S-3)
Senate Bill 151 (Substitute S-2)
Sponsor: Sen. Cameron S. Brown

House Committee: Judiciary
Senate Committee: Technology and Energy

Complete to 5-2-06

A SUMMARY OF SENATE BILLS 53, 54 AND 151 AS PASSED BY THE SENATE 3-9-05

The bills create a new act and amend others to prohibit the unauthorized installation of spyware on computers, and set penalties for the crime.

Senate Bill 151 (S-2) would create the "Spyware Control Act" to prohibit a person who was not an authorized user from willfully—with actual knowledge or with conscious avoidance of actual knowledge—causing computer software to be copied onto a computer in Michigan and using it to do any of the following:

- Deceptively modify settings related to the computer's Internet access or use, collect personal identifying information, or deceptively prevent an authorized user's reasonable efforts to disable or block the reinstallation of software.

- Misrepresent that software would be uninstalled or disabled by an authorized user's action, with knowledge that it would not, or falsely represent that software had been disabled.

- Deceptively remove, disable, or render inoperative security, anti-spyware, or anti-virus computer software.

- Take control of the computer to engage in certain acts.

- Modify security settings for the purpose of stealing personal identifying information or damaging a computer.

The bill would allow the attorney general or an adversely affected person to bring an action against a person for violating the proposed act.

Senate Bill 54 (S-3) would amend Public Act 53 of 1979 (MCL 752.797 et al), which prohibits fraudulent access to computers, computer systems, and computer networks, to prohibit a person from installing or attempting to install spyware into another person's computer or computer system or network, or using or attempting to use spyware,

intentionally and without authorization. The bill also would prohibit a person from manufacturing, selling, or possessing spyware with the intent that it be used in violation of the act. The bill would prescribe criminal penalties for a violation.

Senate Bill 53 (S-2) would amend the Code of Criminal Procedure (MCL 777.17c) to add violations of Senate Bill 54 to the sentencing guidelines. Senate Bill 53 is tie-barred to Senate Bill 54, so that it could not go into effect unless Senate Bill 54 also were enacted.

Each bill is described below in further detail.

Senate Bill 151 (S-2)

Prohibited Activity. The bill would prohibit a person who was not an authorized user from willfully—with actual knowledge or with conscious avoidance of actual knowledge—causing computer software to be copied onto a computer in Michigan and using it to do any of the following:

-- Deceptively modify any of the following settings related to the user's access to or use of the internet: the user's homepage, the default provider or web proxy the user used to gain access to the internet, or the user's bookmarks.
-- Deceptively prevent the user's reasonable efforts to disable or block the reinstallation of software by causing software that the user had properly removed or disabled to reinstall or reactivate automatically without the user's authorization.
-- Misrepresent that software would be uninstalled or disabled by an authorized user's action, with knowledge that it would not.
-- Deceptively remove, disable, or render inoperative security, anti-spyware, or antivirus software installed on the computer.

The bill also would prohibit a person from installing software and using it deceptively to collect personal identifying information that met either of the following criteria:

-- The information was collected through the use of a keystroke-logging function that recorded a user's keystrokes to transfer that information from the computer to another person.
-- If the software were installed in a manner designed to conceal the installation from the user, the information included websites the user visited, other than websites of the software provider.

Additional Prohibitions. A person who was not an authorized user could not, with actual knowledge, with conscious avoidance of actual knowledge, or willfully, cause software to be copied onto a computer in Michigan and use it to take control of the computer by doing any of the following:

-- Transmitting or relaying commercial e-mail or a computer virus from the computer, if the transmission or relaying were initiated by a person other than an authorized user and without the user's authorization.

-- Gaining access to or using an authorized user's modem or internet service for the purpose of causing damage to the computer or causing an authorized user to incur financial charges for a service the user did not authorize.
-- Using the computer as part of an activity performed by a group of computers for the purpose of causing damage to another computer, including launching a denial of service attack.
-- Opening multiple, sequential stand-alone advertisements in the authorized user's Internet browser without the user's authorization and with knowledge that a reasonable user could not close the advertisements without turning off the computer or closing the Internet browser.

The bill also would prohibit a person who was not an authorized user from willfully, with actual knowledge, or with conscious avoidance of actual knowledge, causing software to be copied onto a computer in Michigan and using it modify the following settings related to the computer's access to or use of the internet:

-- An authorized user's security or other settings that protected information about the user, for the purposes of stealing a user's personal identifying information.
-- The computer's security settings, for the purposes of causing damage to one or more computers.

In addition, a person would be prohibited from copying software onto a computer and using it to prevent, without an authorized user's authorization, the user's reasonable efforts to block the installation of, or to disable, software by falsely representing that software had been disabled or by presenting the user with an option to decline installation with knowledge that the installation would proceed even if the user selected that option.

The bill also would prohibit a person who was not an authorized user from inducing an authorized user to install a software component by misrepresenting that the installation was necessary for security or privacy reasons or in order to open, view, or play a particular type of content; or deceptively causing the copying and execution of a computer software component that caused the computer to use the component in a way that violated this provision.

These prohibitions would 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 were 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 the proposed act.

Legal Action. The attorney general or any of the following who was adversely affected by a violation of the proposed act could bring an action against a person for the violation: an authorized user, an Internet website owner or registrant, a trademark or copyright owner, or an authorized advertiser on an Internet website. The person bringing the action could obtain an injunction to prohibit further violations, and/or actual damages sustained by the person, or if the action were brought by the attorney general, by each person adversely affected, or $10,000 per violation, whichever was greater. If the defendant had engaged in a pattern and practice of violating the proposed act, a person could obtain the greater of three times the amount of actual damages, or $30,000 per violation, in addition to an injunction. Additionally, the prevailing party would be entitled to recover the actual costs of the action and reasonable attorney fees incurred.

The bill specifies that a single action or conduct that violated more than one of the bill's provisions would constitute multiple violations of the proposed act. The remedies provided by the bill would be in addition to any other remedies provided by law. Also, a person could not file a class action under the proposed act.

Definitions. The bill would define "authorized user" as the owner of a computer or a person who was authorized by the owner or lessee to use the computer. "Computer software" would mean a sequence of instructions written in any programming language that was executed on a computer. The term would not include a "cookie," which the bill would define as a non-executable text or data file that was used by, or placed on, a computer or computer program, system, or 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, program, system, or network by an authorized user.

Under the bill, "deceptively" would mean by means of any of the following:

-- An intentionally and materially false or fraudulent pretense or statement.
-- A statement or description that omitted or misrepresented material information in order to deceive an authorized user.
-- A material failure to provide any notice to an authorized user regarding the download or installation of software in order to deceive authorized users.

"Personal identifying information" would mean that term as defined in Section 3 of the Identity Theft Protection Act, or a name, number, or other information used as a password or access code. (Under Section 3 of the Identity Theft Protection Act, "personal identifying information" means a name, number, or other information that is used to identify a specific person or provide access to a person's financial accounts, including his or her name, address, telephone number, driver license or state personal identification card number, social security number, place of employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or account

password, stock or other security certificate or account number, credit card number, vital record, or medical records or information.)

Senate Bill 54 (S-3)

Prohibited Activity; Definitions. The bill would prohibit a person from intentionally and without authorization installing or attempting to install spyware into a computer or computer program, system, or network belonging to another person; or using or attempting to use spyware that had been installed on another person's computer, program, system, or network. Additionally, the bill would prohibit a person from manufacturing, selling, or possessing spyware with the intent that it be used to violate Public Act 53 of 1979.

Under the bill, "spyware" would mean computer instructions or a computer program that deceptively monitored, collected, copied, or transferred copies of or was deceptively installed to monitor, collect, copy, or transfer copies of, data or information from or information regarding the use of a computer, or computer program, system, or network, including any of the following:

-- Keystrokes made by an authorized user.
-- Websites the authorized user visited, except websites of the software provider or the originating website location or uniform resource locator automatically sent to the destination website when an authorized user changed websites.
-- Other data or information contained on the computer, system, or network, such as personally identifiable files on a hard drive.

The term would not include conduct by a person acting under a valid legal process within the scope of his or her legal authority, or a "cookie," which would have the same definition as in Senate Bill 151 (S-2). "Spyware" also would exclude all of the following:

-- Monitoring of, or interaction with, an authorized user's Internet or other network or connection service, or computer by a telecommunications carrier, cable operator, computer hardware or software provider, provider of information service, or interactive computer service.
-- For network or computer security purposes, diagnostics, technical support, repair, authorized updates of software, or system firmware.
-- Authorized remote system management.
-- 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 with the reasonable belief that it was installed in violation of the bill.

Penalties. A person who violated the bill would be guilty of a felony punishable by imprisonment for up to five years and/or a maximum fine of $10,000. If the person had a prior conviction, the person would be guilty of a felony punishable by imprisonment for up to 10 years and/or a maximum fine of $50,000. The bill specifies that its provisions

would not prohibit the person from being charged with, convicted of, or sentenced for any other violation of law arising out of the violation of the bill.

Senate Bill 53 (S-2)

The bill would include felony violations of Senate Bill 54 (S-3) in the sentencing guidelines. Installing spyware in a computer, computer system, or computer program would be a Class E property felony punishable by a maximum of five years' imprisonment. Installing spyware with a prior conviction would be a Class D property felony punishable by imprisonment for up to 10 years.

FISCAL IMPACT:

The bills would have an indeterminate fiscal impact, depending on the number of cases brought.

Legislative Analyst: J. Hunault

■ This analysis was prepared by nonpartisan House staff for use by House members in their deliberations, and does not constitute an official statement of legislative intent.