Senate Fiscal Agency
P. O. Box 30036
Lansing, Michigan 48909-7536

BILL ANALYSIS

Telephone: (517) 373-5383
Fax: (517) 373-1986
TDD: (517) 373-0543

Senate Bill 53 (Substitute S-2 as passed by the Senate)
Senate Bill 54 (Substitute S-3 as passed by the Senate)
Senate Bill 151 (Substitute S-2 as passed by the Senate)
Sponsor: Senator Cameron S. Brown
Committee: Technology and Energy

Date Completed: 3-22-05

RATIONALE

It is estimated that 80% to 90% of computers are infected with spyware. According to webroot.com, spyware is any application that may track an individual's online and offline computer activity and is capable of saving that information locally or transmitting it to third parties, often without the user's consent or knowledge. Spyware commonly is installed on a person's computer through a pop-up window or advertisement, in conjunction with the user's downloading of free software, via an instant messenger service, through a file-sharing program, or through spam e-mail or an attachment in an e-mail.

Some spyware programs enable online companies to track a person's activities on a website and tailor pop-up advertising to the person's choices. Other programs are capable of monitoring the person's keystrokes and online screenshots, thus revealing personal information such as login names, passwords, and social security, credit card, and bank account numbers. In addition to creating a nuisance and compromising the security of personal information, spyware can interfere with a computer's performance. Common signs that a computer may be infected with spyware are sluggish performance, increased pop-up ads, unexplained homepage changes, and system crashes. Once installed, spyware can be extremely difficult to remove; often, the computer must be completely reformatted.

Utah and California have enacted antispyware legislation, and a proposal has been introduced in Congress. In light of the problems spyware causes, it has been suggested that Michigan also should prohibit a person from installing the software on another person's computer without permission.

CONTENT

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, antispyware, or antivirus 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, 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 to add violations of Senate Bill 54 (S-3) to the sentencing guidelines.

Senate Bill 53 (S-2) is tie-barred to Senate Bill 54. The bills are 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 the user had properly removed or disable 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, antispyware, 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 nonexecutable 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.

MCL 777.17c (S.B. 53)
752.797 et al. (S.B. 54)

BACKGROUND

Utah's Spyware Control Act

Utah's antispyware legislation was enacted in 2004. The Spyware Control Act prohibits a person from installing spyware, or causing spyware to be installed, on another person's computer; or using a context based triggering mechanism to display an advertisement that partially or wholly covers or obscures paid advertising or other content on an internet website in a way that interferes with a user's ability to view the website. An action against a violator may be brought by any of the following who is adversely affected by the violation: an internet website owner or registrant, a trademark or copyright owner, or an authorized advertiser on an internet website. An adversely affected person may obtain an injunction and/or recover actual damages or $10,000 per violation, whichever is greater, or up to three times the damages allowed if the defendant acted willfully or knowingly. The law also requires Utah's Consumer Protection Division to recommend amendments to the Legislature and establish procedures for consumers to report violations.

Although the new law was supposed to take effect in May 2004, online advertising company WhenU.com filed suit in Utah's Third Judicial District Court, alleging that the Act violates the company's First Amendment right to free speech and unconstitutionally regulates interstate commerce. A judge issued a preliminary injunction in June 2004, preventing the law from taking effect.

In response to the lawsuit, Representative Stephen Urquhart, the sponsor of the original legislation, has introduced House Bill 104 to revise the Act. Rather than prohibit the installation of spyware, the bill would prohibit a person from displaying a pop-up ad via spyware with knowledge or reckless disregard that the ad was displayed in response to a specific trademark or domain name registered in Utah (a "mark") or in response to a specific internet address; and purchased or acquired by a person other than the mark's owner, a licensee or authorized agent of the mark's owner, an authorized user of the mark, or a person advertising the lawful sale, lease, or transfer of products bearing the mark through a secondary marketplace for the sale of goods or services.

The bill also would prohibit a person from purchasing or acquiring advertising delivered in violation of the bill if the person received from the mark owner an actual notice containing a detailed explanation of the violation and the person failed to take reasonable steps to stop the violation.

Under the bill, a person using spyware to display a pop-up ad would not be guilty of a violation if the person first verified that the computer user did not reside in Utah. A person who purchased or acquired advertising would not be guilty of a violation if the person reasonably determined that the person who delivered a pop-up ad by use of spyware had verified that the user did not live in Utah.

The bill also would delete all provisions related to a "context-based triggering mechanism", and would redefine "spyware" as software on the computer of a Utah resident that collected information about a website at the time it was being viewed and used that information to display pop-up advertising. The bill provides that only the Attorney General or a mark owner who did business in Utah and was adversely affected could bring an action against a violator. The bill also would revise the penalties.

Although the Spyware Control Act is in dispute, Utah-based internet retailer Overstock.com filed a lawsuit under the statute in May 2004, against competitor SmartBargains.com for placing pop-up windows advertising SmartBargains' products on Overstock's website without Overstock's authorization.

California's Act

California's Consumer Protection Against Computer Spyware Act took effect on January 1, 2005. The Act is nearly identical to Senate Bill 151 (S-2), except that the California law does not provide for a private cause of action against a violator. Legislation has been introduced to allow a person who has spyware installed or receives software containing spyware in violation of the Act, or the person's internet service provider, to bring an action against the violator. Under the bill, the person bringing the action could recover either actual damages, or liquidated damages of $1,000 for each instance of spyware or software containing spyware installed, or both, in addition to reasonable attorney fees and costs. The bill also provides that a violation of the Act would be a crime punishable as either a misdemeanor or a felony.

Federal Legislation

Congresswoman Mary Bono has introduced H.R. 29 to create the "Securely Protect Yourself Against Cyber Trespass Act" ("SPY ACT"). Under the bill, it would be unlawful for any person who was not the owner or authorized user of a protected computer to engage in deceptive acts or practices that involved any of the following:

-- Taking control of the computer by certain actions (e.g., using the computer to send unsolicited information from it to others, or diverting the internet browser without the computer owner's or user's authorization and away from the site the user intended to view).
-- Modifying settings related to the use of the computer, or to its access to or use of the internet by altering the user's homepage, default provider or other existing internet connections settings, bookmarks, or security or other settings that protected information about the owner or authorized user for the purpose of causing damage or harm to the computer, owner, or user.
-- Collecting personally identifiable information through the use of a keystroke logging function.
-- Inducing the owner or authorized user to install a computer software component, or preventing reasonable efforts to block the installation of or to disable a software component, by taking certain actions.
-- Misrepresenting that installing a separate software component or providing log-in and password information was necessary for security or privacy reasons.
-- Inducing the owner or authorized user to install or execute software by misrepresenting the identity or authority of the person providing the software.
-- Inducing the owner or authorized user to provide personally identifiable, password, or account information to another person by misrepresenting the identity of the person seeking the information or without the intended recipient's authority.
-- Removing or disabling a security, antispyware, or antivirus technology installed on a computer.
-- Installing or executing additional software components to cause a person to use them in a way that violated any other provision of the bill.

In its discretion, the Federal Trade Commission (FTC) could seek a civil penalty of up to $3.0 million for a violation of this prohibition.

The bill also would make it unlawful to transmit to a protected computer any information collection program or to execute any information collection program installed on a protected computer, unless the program provided notice before execution of any of the information collection functions and included specific required functions. The notice would have to state that the program would collect and transmit information about the user or about websites the user visited and use that information to display advertising. The notice would have to provide for the user to grant or deny consent and to abandon or cancel the transmission or execution without granting or denying consent. For a violation of those provisions, the FTC could seek a civil penalty of up to $1.0 million.

The bill would exempt from liability a telecommunications carrier, an information service or interactive computer service provider, a cable operator, or transmission capability provider in performing its duties. The SPY ACT would not apply to any action taken by a law enforcement agent in the performance of official duties, or the transmission or execution of an information collection program in compliance with a law enforcement, investigatory, national security, or regulatory agency or department of the United States or any state in response to a request or demand made under authority granted to that agency or department. The bill also includes other security-related exceptions.

The bill would supersede any provision of a statute, regulation, or rule of a state or political subdivision of a state that expressly regulates deceptive conduct with respect to computers similar to that described in the bill, the transmission or execution of a computer program similar to that described in the bill, or the use of computer software that displays advertising content based on the websites viewed using a computer. Additionally, no person other than the Attorney General of a state could bring a civil action under the law of any state if the action were premised upon the defendant's violating any provision of the proposed SPY ACT.

The SPY ACT would not apply after December 31, 2010.

(This summary of the proposed SPY ACT reflects the legislation as it was introduced. The bill was approved by the House Energy and Commerce Committee's Subcommittee on Commerce, Trade and Consumer Protection on February 16, 2005, with several technical amendments.)

FTC Litigation

In October 2004, the FTC filed a complaint in United States District Court for the District of New Hampshire against Seismic Entertainment Productions and Smartbot.net, alleging that the companies had violated the FTC Act, which prohibits unfair or deceptive acts or practices in or affecting commerce. The complaint stated that the defendants exploited vulnerabilities in certain versions of the Microsoft Internet Explorer web browser to install software without the users' knowledge or authorization. The software would change the users' homepages, modify web browsers' search engines, download and install various advertising and other software programs, redirect users to websites they did not intend to visit, and cause an incessant stream of pop-up ads. The complaint alleged that the defendants' practices caused consumers' computers to malfunction, slow down, or crash, and that some consumers had lost data stored on their computers.

The FTC also stated in its complaint that Seismic and Smartbot.net had marketed supposed "anti-spyware" software through pop-up ads it displayed to visitors to internet websites under their control. The ads would warn users that their computers were infected with spyware, and advise that they immediately should click on a provided link to purchase an antispyware program.

The FTC claimed that consumers had to spend substantial time and money to resolve problems the defendants caused by changing their web browsers and installing software without authorization, and unfairly compelling them to purchase antispyware software. The complaint alleged that the consumers could not reasonably avoid this substantial injury, and it was not outweighed by benefits to consumers or competition. Therefore, the defendants' practices were unfair and in violation of the FTC Act.

The FTC requested the Court to issue a preliminary injunction. The Commission further requested that the court permanently enjoin the defendants from violating the FTC Act; award equitable relief to redress injury to consumers, including rescission of contracts and restitution, and the disgorgement of ill-gotten gains; and award the FTC the costs of bringing the action and any additional relief the Court determined just and proper. The Court issued a preliminary injunction in December 2004.

ARGUMENTS

(Please note: The arguments contained in this analysis originate from sources outside the Senate Fiscal Agency. The Senate Fiscal Agency neither supports nor opposes legislation.)

Supporting Argument

Along with vast capabilities for communication and information, the internet provides increased opportunities for unscrupulous people to exploit others' vulnerabilities. Most people have a reasonable expectation that the activities in which they engage in their own homes will remain private. At best, spyware can be annoying. At worst, it can create technical problems that may be time-consuming and costly to resolve, as well as aid people who want to obtain and use other people's personal information for their own benefit. The surreptitious software results in reduced productivity for businesses and can undermine consumers' confidence in the online marketplace. Whether it is merely a nuisance or used for malicious purposes, spyware amounts to an invasion of privacy.

The bills would help eliminate spyware by proscribing unacceptable uses of software designed to take control of a computer or track a user's activities. In order to use spyware legally, companies simply would have to refrain from using deceptive or fraudulent tactics to install it, or installing it for illicit purposes. Many legitimate businesses that currently use spyware would stop because they would not want to operate outside of the law. Companies or individuals who continued to use spyware illegally would be more identifiable, which would make it easier to take civil action against them or criminally prosecute the worst offenders.

Opposing Argument

The bills would prohibit certain actions, such as using another person's computer to transmit a virus or as part of a denial of service attack, that already may be addressed under existing computer crime, fraud, and unfair trade practice laws. For example, the Michigan Attorney General and the FTC already may take action against entities that engage in unfair or deceptive business practices, as the FTC did last year against Seismic Entertainment and Smartbot.com. At the same time, the bills would fail to address other questionable but legal tactics that purveyors of spyware use to confuse or deceive customers into installing their software. For example, the bills omit notice and consent standards for software installation. According to Harvard spyware researcher Ben Edelman, online marketing company Claria sometimes "notifies" consumers in a 5,500-word, 56-page end-user license agreement (EULA) that, by downloading certain software, the user also agrees to the installation of Claria's software, which delivers periodic advertising. Other times, the company allegedly displays the EULA only after the consumer unwittingly has accepted installation of the software. In failing to prohibit these "drive-by" software installations, the bills implicitly would approve such tactics and lend the appearance of legitimacy to businesses that use them.

A patchwork of state laws could create an excessive compliance burden on companies that simply wish to advertise online. Rather than relying on the government to solve the problem of spyware, consumers should depend on the information technology industry itself. Competition will force businesses to continue improving antispyware software, making their products more attractive to potential customers. Many companies already sell programs to cleanse computers of unwanted software, and Microsoft recently announced that it will give antispyware programs away for free.

Response: Spyware is a growing problem, despite the availability of software to combat it and the FTC's enforcement authority under the FTC Act. It is difficult to identify and remove all the unwanted software installed on a computer, even with multiple antispyware programs working simultaneously. Furthermore, the FTC has filed only one spyware complaint. The bills would provide another tool, in addition to technological solutions offered by the private sector and penalties authorized under existing law.

Opposing Argument

No law, no matter how well-crafted, will solve the problem of spyware completely. The internet is a global medium, and, as with spam, many of the bad actors are outside the jurisdiction of Michigan or the United States. Despite the enactment of Federal antispam legislation, which took effect on January 1, 2004, the amount of spam continues to grow. It is likely that antispyware legislation similarly would be difficult to enforce.

Response: Although many people who misuse the internet live outside the reach of State or Federal laws, the bills would provide for civil and criminal penalties against those who are located here. Furthermore, spam

operations typically are run by one person, often out of his or her home, and are difficult to find and stop. Spyware companies, however, frequently are established businesses that cannot hide their identities as readily and would be easier to catch and penalize.

Legislative Analyst: Julie Koval

FISCAL IMPACT

Senate Bill 151 (S-2)

The bill would have an indeterminate impact on the Department of Attorney General, depending on the number of cases that would be filed under this legislation.

Senate Bills 53 (S-2) and 54 (S-3)

The bills would have an indeterminate fiscal impact on State and local government. There are no data to indicate how many offenders would be convicted of the proposed crimes. An offender convicted of the Class E offense would receive a sentencing guidelines minimum sentence range of 0-3 months to 24-38 months. An offender convicted of the Class D offense would receive a sentencing guidelines minimum sentence range of 0-6 months to 43-76 months. Local units would incur the costs of misdemeanor probation and incarceration in a local facility, both of which vary by county. The State would incur the cost of felony probation at an average annual cost of $2,000, as well as the cost of incarceration in a State facility at an average annual cost of $28,000.

Fiscal Analyst: Bill Bowerman
Bethany Wicksall

A0506\s53b