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-1 as reported)
Senate Bill 54 (Substitute S-1 as reported)
Senate Bill 151 (Substitute S-1 as reported)
Sponsor: Senator Cameron S. Brown
Committee: Technology and Energy

Date Completed: 2-28-05

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-1) would create the "Spyware Control Act" to do the following:

-- Prohibit a person from installing spyware on another person's computer, or causing spyware to be installed on another person's computer.
-- Prohibit a person from using a context-based triggering mechanism to display an advertisement that covered content on a website in a way that interfered with a user's ability to view the internet.
-- 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-1) 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 on another person's computer without permission, and prescribe criminal penalties for a violation.

Senate Bill 53 (S-1) would amend the Code of Criminal Procedure to add

violations of Senate Bill 54 (S-1) to the sentencing guidelines.

Senate Bill 53 (S-1) is tie-barred to Senate Bill 54. The bills are described below in further detail.

Senate Bill 151 (S-1)

Prohibited Activity; Definitions

The bill would prohibit a person from installing spyware on another person's computer or causing spyware to be installed on another person's computer. The bill also would prohibit a person from using a context-based triggering mechanism to display an advertisement that wholly or partially covered or obscured paid advertising or other internet website content in a way that interfered with a user's ability to view the internet.

The bill would define "spyware" as software residing on a computer that collected protected information and sent the information to a remote computer or server, and/or displayed or caused to be displayed in response to protected information an advertisement to which any of the following applied:

-- The advertisement did not identify clearly the full legal name of the entity responsible for delivering it.
-- The advertisement used a Federally registered trademark as a trigger for its display by a person other than the trademark owner or the owner's authorized agent or licensee, or a recognized internet search engine.
-- The advertisement used a triggering mechanism to display the advertisement based on the internet websites the computer accessed.
-- The advertisement was displayed using a context-based triggering mechanism and partially or wholly covered or obscured paid advertising or other content on a website in a manner that interfered with the computer user's ability to view the website.

"Context-based triggering mechanism" would mean a software-based trigger or program residing on a computer that displayed an advertisement based on either the internet website to which the computer gained access, or the website's contents or characteristic.

"User" would mean a computer owner or a person who gained access to an internet website.

"Protected information" would mean the internet websites accessed with the computer; the contents or characteristics of the websites; and/or personal information entered or revealed during the computer's operation, including all of the following:

-- An individual's first and last name, whether given at birth or adoption, assumed, or legally changed.
-- An individual's street name, city or town, zip code, or physical address.
-- An e-mail address.
-- A telephone number.
-- A social security, personal identification, or credit card number, or access code associated with a credit card.
-- A date or place of birth or birth certificate number.
-- A password or access code.

Additionally, "protected information" would include information submitted via forms on an internet website.

The bill specifies that the term "spyware" would not include software designed and installed solely to diagnose or resolve technical difficulties. The term also would exclude software or data that reported to an internet website information previously stored by the website on the computer, including cookies, HTML code, Java scripts, and a computer operating system.

The term "spyware" would not include software for which all of the following were obtained:

-- A license agreement for the software that was presented in full and written in plain English.
-- A notice of the collection of each specific type of information to be transmitted as a result of the software installation.
-- A clear and representative full-sized example of each type of advertisement that could be delivered as a result of the software installation.
-- A truthful statement of the frequency with which each type of advertisement

could be delivered as a result of the software installation.

-- For each type of advertisement delivered as a result of the software installation, a clear description of a method by which a user could distinguish the advertisement by its appearance from an advertisement generated by other software services.

-- A method by which the computer user quickly and easily, using obvious, standard, usual, and ordinary methods, could disable and remove the software with no other effect on the nonaffiliated parts of the computer.

Exemption from Prohibition

The prohibition against installing spyware, or using a context-based triggering mechanism that interfered with a user's ability to view the internet, would not apply to monitoring of or interaction with a subscriber's internet or other network connection or service, or a protected computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service for network or computer security purposes, diagnostics, technical support, repair, authorized updating of software or system firmware, 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 installed on a computer in violation of the proposed Act.

The bill would define "protected computer" as it is defined in 18 USC 1030, which defines the term as a computer exclusively for the use of a financial institution or the United States government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the U.S. government and the conduct constituting the offense affects that use by or for the financial institution or the government; or a computer that is used in interstate or foreign commerce or communication, including a computer located outside the U.S. that is used in a manner that affects interstate or foreign commerce or communication of the U.S.

"Information service" would mean that term as defined in 47 USC 153. Under that section, the term means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.

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: a 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. For a knowing violation, a person could obtain the greater of three times the amount of actual damages, or $30,000 per violation, in addition to an injunction.

The bill specifies that each instance of obtaining access to user information and each display of an advertisement would be a separate violation of the proposed Act. It would not be a defense to an action that a user could remove or hide spyware or an advertisement.

The bill provides that it would not authorize a person to file an action against an internet service provider for the routine transmission of security information, or information that contained an advertisement in violation of the proposed Act. Also, a person could not file a class action under the proposed Act.

Senate Bill 54 (S-1)

Prohibited Activity

The bill would prohibit a person from installing or attempting to install spyware into a computer program, computer, computer system, or computer network belonging to another person unless all of the following applied:

-- The person provided his or her name and business address and a valid telephone number, e-mail address, or internet service provider address where he or she could be reached, or, if the spyware were to be installed on behalf of another person, where that other person could be reached.
-- The person provided specific notice of the intent to install the spyware.
-- If applicable, the person specifically stated that a fee was to be charged or could be incurred and the amount of the fee.
-- If applicable, the person specifically stated the information that was to be obtained from the computer or the computer program, system, or network.
-- If applicable, a statement that sexually explicit material would be displayed.
-- The owner or person responsible for maintaining the computer, program, system, or network affirmatively granted the right to install the spyware.

The notice of intent to install spyware would have to include a statement that instructions or software would be downloaded into the computer program, computer, computer system, or computer network, and how the instructions or software were intended to affect the operation of the program, computer, system, or network. The notice also would have to provide a method by which the owner or person responsible for maintaining the program, computer, system, or network could refuse installation and require that no further contact be made regarding the installation of spyware.

If the right to install spyware were authorized, the person installing the spyware could not exceed the nature or the scope of the authorization granted. A person could not contact subsequently a person who informed him or her that no further contact was to be made.

The bill also would prohibit a person from manufacturing, creating, distributing, or possessing spyware to be used in violation of the bill's provisions.

Penalties

A person who violated the bill would be guilty of a misdemeanor punishable by imprisonment for up to 93 days and/or a maximum fine of $1,000. If the violation caused interruption of or interference to the use of the computer program, computer, computer system, or computer network, the person would be guilty of a felony punishable by imprisonment for up to two years and/or a maximum fine of $5,000. If a person had a prior conviction, he or she would be guilty of a felony punishable by imprisonment for up to four years and/or a maximum fine of $10,000.

Exemptions

The bill would not apply to monitoring of or interaction with a subscriber's internet or other network connection or service, or a protected computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service for network or computer security purposes, diagnostics, technical support, repair, authorized updating of software or system firmware, 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 installed on a computer in violation of the bill.

Definition of "Spyware"

Under the bill, "spyware" would mean computer instructions or software installed into a computer program, computer, computer system, or computer network for any of the following purposes:

-- Monitoring the use of a computer program, computer, computer system, or computer network.
-- Sending information about the use of a computer program, computer, computer system, or computer network to a remote computer, server, or data collection site or point.
-- Displaying an advertisement or causing an advertisement to be displayed in response to the use of a computer program, computer, computer system, or computer network.

The term would not include any of the following:

-- Computer instructions or software installed by the manufacturer of the

computer program, computer, computer system, or computer network that was intended to facilitate ordinary and expected access to and use of the program, computer, system, or network.
-- Computer instructions or software installed by the owner of a computer program, computer, computer system, or computer network, except as otherwise provided in the bill.
-- Computer instructions or software installed by a person maintaining a computer program, computer, computer system, or computer network on behalf of the owner while acting within the scope of his or her authority.
-- An ISP acting within the scope of its authority.
-- A person authorized by law to conduct criminal investigations while acting within the scope of his or her authority.
-- Instructions commonly known as cookies that were intended solely to facilitate recognition of the computer for internet access or use.

Senate Bill 53 (S-1)

The bill would include felony violations of Senate Bill 54 (S-1) in the sentencing guidelines. Installation or attempted installation of spyware causing interruption or interference would be a Class G property felony punishable by a maximum of two years' imprisonment. Installation or attempted installation with a prior conviction would be a Class F property felony punishable by imprisonment for up to four years.

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

BACKGROUND

Utah's Spyware Control Act

Utah's anti-spyware legislation was enacted in 2004. Utah's law is nearly identical to Senate Bill 151, except that it does not provide for an action to be brought against a violator by the Attorney General, and it limits a person's recovery to three times the amount of actual damages. The law also requires Utah's Consumer Protection Division within the Department of Commerce 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.

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.

In response to the WhenU.com 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.

California's Act

Under the Consumer Protection Against Computer Spyware Act, a person or entity who is not an "authorized user" (i.e., a person who owns or is authorized by the owner or lessee to use a computer) may not knowingly or willfully cause computer software to be copied onto the computer of a California consumer and use the software to do any of the following:

-- Modify, through intentionally deceptive means, a user's homepage, default provider or Web proxy, or list of bookmarks.
-- Collect, through intentionally deceptive means, personally identifiable information that meets specific criteria.
-- Prevent, without the user's authorization, through intentionally deceptive means, a user's reasonable efforts to block the installation of or disable software by causing the software automatically to reinstall or reactivate on the computer.
-- Intentionally misrepresent that software will be uninstalled or disabled by a user's action.
-- Remove, disable, or render inoperative security, antispyware, or antivirus software installed on the computer through intentionally deceptive means.

The Act also prohibits a person or entity that is not an authorized user from knowingly or willfully causing computer software to be copied onto a consumer's computer and using the software to do any of the following:

-- Take control of the consumer's computer by certain actions (e.g., transmitting commercial e-mail or a computer virus from the computer).
-- Modify an authorized user's security settings for the purpose of stealing personal information or causing damage to the computer.
-- Prevent an authorized user's reasonable efforts to disable or block the installation of software.

In addition, the Act prohibits a person who is not an authorized user from inducing an authorized user to install a software component onto the computer by intentionally misrepresenting that installing software is necessary for security or privacy reasons or to gain access to a particular type of content.

Federal Legislation

Congresswoman Mary Bono 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 act 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 defining spyware and proscribing unacceptable uses of software designed to track a computer user's activities. Many legitimate businesses that currently use spyware would stop because they would not want to operate outside of the law. In order to use spyware legally, companies simply would have to notify consumers and obtain their consent before installing the software, and provide a mechanism to remove it. 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

Although alleviating the problems caused by spyware is a worthwhile endeavor, Senate Bill 151 (S-1) contains some constitutional issues that should be addressed. Last year, a Utah judge granted an injunction against that state's antispyware law, after which the bill is modeled, on the grounds that it violated a company's right to advertise and regulated interstate commerce. The sponsor of that legislation has introduced some substantive amendments this session so that the law will withstand legal scrutiny. Perhaps California's law would be a more appropriate and effective model for Michigan.

Opposing Argument

The legislation is overly regulatory and unnecessary. First, the definitions of "spyware" in Senate Bills 151 (S-1) and 54 (S-1) are too broad. Senate Bill 151 (S-1) would prohibit pop-up ads from being displayed over other ads or websites, even if the user authorized them, and Senate Bill 54 (S-1) would prohibit ads from being displayed in response to a specific website. Additionally, programs parents use to monitor the websites their children visit could fall under the proposed definitions of spyware. Other software, known as "supportware", that benefits users by providing security patches and updates to computer operations also could be considered "spyware" under the bills. Second, the FTC already may take action under the FTC Act against entities that engage in unfair or deceptive business practices, as it did last year against Seismic

Entertainment and Smartbot.com. Furthermore, a patchwork of state laws could create an excessive compliance burden for legitimate 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: The bills simply would require that a user be notified and given a chance to accept or decline the installation of software. It is not likely that the producers of genuinely beneficial "supportware" would install a program on a person's computer without authorization. Additionally, the bills would make exceptions for programs used in diagnostics and troubleshooting, and to remove unwanted programs.

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 Federal 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.

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-1)

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-1) and 54 (S-1)

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 G offense would receive a sentencing guidelines minimum sentence range of 0-3 months to 7-23 months. An offender convicted of the Class F offense would receive a sentencing guidelines minimum sentence range of 0-3 months to 17-30 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\s53a