

CHILD PROTECTION REGISTRY

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

House Bill 5979 as enrolled
Public Act 242 of 2004
Sponsor: Rep. David Palsrok

Senate Bill 1025 as enrolled
Public Act 241 of 2004
Sponsor: Sen. Michael D. Bishop
House Committee: Energy and Technology
Senate Committee: Technology and Energy

Second Analysis (12-29-04)

BRIEF SUMMARY: Senate Bill 1025 would create the Michigan Children's Protection Registry Act as a means of preventing minors from being sent a message that advertises or otherwise links to a message that advertises a product or service that a minor is prohibited by law from purchasing, viewing, possessing, or otherwise receiving. House Bill 5979 would amend Public Act 53 of 1979 dealing with computer crimes to make violations of the registry act also violations of Public Act 53 and to prescribe penalties. The two bills were tie-barred, meaning that neither would take effect unless both were enacted.

FISCAL IMPACT: The bills would have an indeterminate impact on the State or on local units of government. It is difficult to determine how many potential violators may be convicted or how much the Department of Labor and Economic Growth may receive in fee revenue. With the ability by the Department to set the fee structure for individuals desiring to communicate via the registry it could be assumed that creation and maintenance of the registry may be self-supporting financially.

THE APPARENT PROBLEM:

As the use of e-mail as a critical mode of communication has increased, so has the practice of "spamming", in which an e-mail marketer (or "spammer") sends unsolicited advertising to millions of people. Reportedly, between 40 percent and 50 percent of all e-mail sent is spam. Spammers apparently do not limit themselves to e-mail, however, but also send unsolicited advertisements to users of instant messaging services and to mobile phones in the form of text messages. A significant portion of spam is said to contain pornography or other material that is inappropriate for children. Although anti-spam legislation (described under Background Information, below) recently has been enacted both in Michigan and at the federal level, some people believe that a special registry should be created in order to prevent messages containing sexual content or advertisements for gambling, cigarettes, and alcohol from reaching children.

THE CONTENT OF THE BILLS:

Taken together, the bills would 1) create the Michigan Children's Protection Registry Act as a means of preventing minors from being sent electronic messages that advertise or otherwise link to messages that advertise products or services that minors are prohibited from purchasing, possessing, viewing, or otherwise receiving; and 2) create computer crime penalties for violations of the new registry act. The two bills were tie-barred, meaning neither could take effect unless both were enacted. Both would take effect July 1, 2005.

Senate Bill 1025

The bill would create the "Michigan Children's Protection Registry Act" to do the following:

-- Require the Department of Labor and Economic Growth (DLEG) to establish and operate a "Child Protection Registry" on which a person or school could register contact points (e.g., e-mail addresses) belonging to a minor or to which a minor could have access. Alternatively, the department could contract with a qualified third party to establish and operate the registry. A registration would be for no more than three years (although it could be renewed) and would expire when the minor turned 18 years of age. Schools and other institutions serving minors could make one registration to register multiple contact points. There could be no fee or charge for an individual or entity registering a contact point. The registry would have to be fully operational by July 1, 2005. It would not be subject to the Freedom of Information Act.

-- Prohibit a person from sending, causing to be sent, or conspiring to send a message to a registered contact point that had been registered for more than 30 calendar days if the primary purpose of the message was, directly or indirectly, to advertise or otherwise link to a message that advertised a product or service that a minor is prohibited by law from purchasing, viewing, possessing, participating in, or otherwise receiving. The consent of a minor or third party to receive a message would not be a defense to a violation. However, it would not be a violation for a person to be an intermediary between the sender and recipient in a transmission. The sending of a message would only be prohibited if it was otherwise a crime for the minor to purchase, view, possess, or otherwise receive the product or service.

-- Specify that a violation of the act would be a computer crime and would be a violation of Public Act 53 of 1979 subject to the penalties of that act (as described later).

-- Require a person who wanted to send such a communication to pay a fee set by DLEG to verify compliance with the registry. The fee could not exceed .03 cents per contact point checked. DLEG would have to establish a mechanism for senders to verify compliance with the registry.

-- Dedicate 85 percent of the fees collected to the new Children's Protection Registry Fund (described later) and 15 percent to the attorney general for investigation and enforcement.

-- Prohibit the release of information contained on the registry or provide access to contact points or other information (except as specifically permitted). Further, a person would be prohibited from accessing or attempting to access the registry except as provided in the act. A person also could not sell or use the registry for any reason other than to meet the new act's requirements.

-- Allow civil actions based on the computer crimes established in the new act to be brought by an authorized individual or the registrant of the contact points on behalf of the minor who has received a message; by a person through whose facilities the message was transmitted; and by the attorney general. The prevailing party in a civil action could recover actual damages, including reasonable attorney fees; or, in lieu of actual damages the lesser of 1) \$5,000 per message received by a recipient or transmitted or 2) \$250,000 for each day a violation occurred. Civil penalties collected by the attorney general would be credited to the attorney general for the costs of investigating and enforcing the new act and the criminal penalties added to Public Act 53 of 1979.

-- Allow the attorney general to investigate the business transactions of a person believed to have violated the act. The AG could require the person to appear at a reasonable time and place to give information under oath and to produce documents and evidence necessary to determine if the person was in compliance with the new act.

-- Create the "Children's Protection Registry Fund" as a separate fund within the Department of Treasury to be administered by DLEG. The fees, fines, and civil penalties collected under the act would have to be deposited into the fund. The department could spend money from the fund only for the purposes of administering the registry. Money in the fund at the end of a fiscal year would remain in the fund and not revert to the General Fund.

The bill would define a "contact point" as any electronic identification to which messages could be sent, including an electronic mail (e-mail) address; an instant message identity; a wireless telephone, personal digital assistant, or similar wireless communication; a facsimile number, or other electronic addresses subject to rules promulgated under the proposed act by DLEG.

House Bill 5979

The bill would amend Public Act 53 of 1979 dealing with computer crimes (MCL 752.795a, et al.) to make violations of the Michigan Children's Protection Registry Act also violations of Public Act 53 and to prescribe penalties. The new registry act would be created by Senate Bill 1025 as a means of preventing minors from being sent an electronic message that advertises or otherwise links to a message that advertises a

product or service that a minor is prohibited by law from purchasing, viewing, possessing, or otherwise receiving.

Under House Bill 5979, a first offense would be a misdemeanor punishable by imprisonment for not more than one year and/or a fine of not more than \$10,000. A second offense would be a felony punishable by imprisonment for not more than two years and/or a fine of not more than \$20,000. A third or subsequent offense would be a felony punishable by imprisonment for not more than three years and/or a fine of not more than \$30,000.

A money and other income and all computer equipment, computer software, and personal property used in connection with a violation and know by the owner to be used in connection with a violation would be subject to lawful seizure and forfeiture as provided under the Revised Judicature Act.

It would be a defense that a communication was transmitted accidentally; the burden of proving the transmission was accidental would be on the sender. The bill specifies that a person would not violate the act solely by being an intermediary between the sender and recipient in the transmission of communication that violated the act or by unknowingly transmitting electronic messages in violation of the act.

BACKGROUND INFORMATION:

Some of the information in this analysis, including the background information that follows, is derived from the Senate Fiscal Agency's analysis of the Senate-passed version of Senate Bill 1025 dated 5-25-04

State Legislation. Public Act 42 of 2003 (House Bill 4519) created the "Unsolicited Commercial E-mail Protection Act" to regulate e-mail messages that contain advertisements and are sent without the recipient's express opinion. The act took effect on September 1, 2003. Under the act, senders of unsolicited commercial e-mail must identify themselves truthfully, include in the subject line the letters "ADV:" to identify the message as an advertisement, and provide a convenient, free way for recipients to opt out of receiving future e-mails.

Additionally, the act prohibits a sender from misrepresenting or failing to include information necessary to identify the e-mail's point of origin or transmission path; using a third party's domain name or e-mail address in identifying the point of origin or transmission path without the third party's consent; and providing another person with software designed to falsify transmission information.

A violation of the act is a misdemeanor punishable by imprisonment for up to one year and/or a maximum fine of \$10,000. A person who violates the prohibitions relating to the disclosure of transmission information, or violates the act in furtherance of another crime, is guilty of a felony punishable by imprisonment for up to four years and/or a maximum fine \$25,000. In addition, a recipient of an e-mail sent in violation of the act, an e-mail

service provider through whose facilities the e-mail was sent, or the attorney general may bring a civil action against a sender. The recipient, service provider, or attorney general may recover actual damages, or the lesser of either \$500 per e-mail received or \$250,000 for each day the violation occurred. The prevailing recipient or service provider also must be awarded actual costs and reasonable attorney fees.

Federal Legislation. President George W. Bush signed the CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) Act into law in December 2003. The law authorizes the Federal Trade Commission (FTC) to create a "Do Not E-Mail" registry. Similar to the state legislation, it requires senders to include an opt-out mechanism for recipients, and prohibits spammers from providing deceptive information about their identities. The law also prohibits false or misleading subject lines, and requires a sender to identify the message as an advertisement or a solicitation and, if applicable, to indicate that it contains sexually oriented material. Additionally, the law prohibits spammers from "harvesting" multiple e-mail addresses from web sites. It allows the FTC, state attorneys general, and Internet service providers to bring actions against violators, and provides for a penalty of imprisonment for up to five years under certain circumstances. Unlike Michigan's law, the CAN-SPAM Act does not contain a private right of action for recipients.

As required by the act, the Federal Trade Commission promulgated a rule under which spam that contains sexually oriented material must include the warning "SEXUALLY-EXPLICIT:" in the subject line. The rule took effect on May 19, 2004.

ARGUMENTS:

For:

As the number of unsolicited and often unwanted electronic messages (known as spam) increases, so does the potential that a child will be exposed to inappropriate material. According to Unspam, an advocacy organization for effective anti-spam laws, 80 percent of children online report receiving inappropriate unsolicited e-mail messages on a daily basis. In addition, it is estimated that 791 million text messages containing sexual content will be sent to cell phones in the United States by 2007, and approximately 60 percent of teenagers in this country already have cell phones. Marketing "adult" material via electronic means is an easy way for spammers to make a profit, as potential customers no longer must deal with the embarrassment of having others see them go behind a curtain to obtain pornography.

Anti-spam laws enacted in several states have proven largely ineffective because they do not provide the state with jurisdiction to prosecute a person who violates the law from another state or country. Even under the federal CAN-SPAM Act, a spammer can continue sending unsolicited e-mail as long as he or she labels the message as spam in the subject line, supplies truthful sender identification, and provides a method for the recipient to opt out of receiving future e-mails. The act does not actually prohibit spam, nor does it provide any protection specifically for children or provide for a private cause of action against a violator. Under Senate Bill 1025, however, a newly created registry

would make it clear which contact points were off limits to spammers and provide the state with jurisdiction, which is critical to prosecuting a violator.

Because many children grow up with cell phones and computers, they often are more adept at using technology than their parents. They should not be subjected to advertisements for drugs and gambling, or pornographic material, while using computers for appropriate purposes, such as doing homework, playing games, and chatting online with friends. The bill would help reduce the number of harmful images sent electronically and provide parents with a tool to protect their children in a technological world.

Against:

While the bills are well-intentioned and may indeed prove to be a useful method of protecting children for inappropriate and harmful communications, a cautionary note is appropriate. Testimony from the state officials who will have to police and enforce this act suggests that the state could face serious difficulties in implementing the new act. There will likely be legal challenges on several fronts, including First Amendment arguments against regulating speech, arguments over the state's jurisdiction over out-of-state violators, and issues of federal pre-emption of spam regulation. There are also concerns about how effectively the state can pursue violators, who may be hard to trace. Enforcement could prove extremely challenging, and both time-consuming and expensive.

Response:

The bills have been drafted in anticipation of such challenges. Note that they now treat transmissions as computer crimes and address improper commercial speech. They also permit private rights of action against violators. While there may be challenges in enforcing this kind of law, the bills take a step in the right direction, and certainly the effort is worth making.

Legislative Analyst: Chris Couch
Fiscal Analyst: Steve Stauff

■ 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.