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 357 (Substitute S-7 as passed by the Senate)
Sponsor: Senator Michael D. Bishop
Committee: Technology and Energy

Date Completed: 7-2-03

RATIONALE

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. According to a representative of EarthLink, an internet service provider (ISP), the amount of spam sent through its services increased 500% over an 18-month period. Unlike the junk mail sent through the traditional postal service, bulk e-mail is sent at minimal cost to the sender. Consumers, however, pay higher prices in the long run for more bandwidth, technicians, and filtering software, and businesses experience losses in productivity. For example, a representative of Spartan Stores said that the company receives 20,000 spam e-mails every week. According to the Michigan Manufacturers Association, the total cost to businesses is about $1 per spam e-mail.

Reportedly, between 40% and 50% of all e-mail sent is spam, a large portion of which is in some way deceptive or fraudulent. Spammers continue to find ways around filtering software, which is typically about 70% effective. Furthermore, in an effort to cast a broad net in catching spam, filters often screen out legitimate e-mail the recipient would have wanted to read. Not only is it time consuming for recipients to wade through the unsolicited e-mails, many of the e-mails evidently contain pornography or other material that is inappropriate for children.

Some people believe that creating a State e-mail registry similar to the "Do-Not-Call" list, requiring spammers to provide contact information and clearly identify their e-mails as advertising, and prescribing civil and criminal penalties against people who send unsolicited e-mail to people who do not want it, would help alleviate the problems caused by spam.

CONTENT

The bill would create the "Electronic Mail Solicitation Act" to do all of the following:

-- Create the Electronic Mail Solicitation Program within the Department of Consumer and Industry Services (DCIS) and require the Program to maintain a list of e-mail addresses of people who did not want to receive unsolicited commercial e-mail.
-- Provide that the Program would be funded by the fees, fines, civil penalties, and forfeitures collected by the Attorney General for violations of the Act.
-- Require senders of unsolicited commercial e-mail to register with the Program and pay a fee.
-- Require senders to include a valid method for recipients to opt out of receiving future e-mail.
-- Require certain information to be included in an unsolicited commercial e-mail.
-- Prohibit a sender of unsolicited commercial e-mail from using a third party's internet domain name or e-mail address without consent; or misrepresenting or failing to include information in identifying the point of origin or the transmission path of the e-mail.
-- Prohibit a person from knowingly selling, giving, or otherwise distributing or possessing with the intent to sell, give, or distribute software designed to facilitate or enable the falsification of e-mail

transmission information or other routing information; or providing such software directly or indirectly to another person.

-- Require a sender of unsolicited commercial e-mail to establish and maintain the necessary policies and records to ensure that a recipient who notified the sender that he or she did not wish to receive future e-mail did not receive any e-mail from the date of notice.

-- Allow an e-mail service provider to design its software so that a sender of unsolicited commercial e-mail was notified of the bill's requirements each time the sender requested delivery of e-mail.

-- Prescribe criminal penalties for violating the proposed Act, and allow a recipient, an e-mail service provider, or the Attorney General to bring a civil action against a violator.

Under the bill, "unsolicited" would mean without the recipient's express permission. An e-mail would not be unsolicited if the sender had a preexisting business or personal relationship with the recipient, or if the e-mail were received because the recipient opted into a system in order to receive promotional material. ("Preexisting business relationship" would mean that there was a business transaction between the initiator and the recipient of a commercial e-mail message during the 10-year period preceding the receipt of that message. The term would include a transaction involving the free provision of information, goods, or services requested by the recipient.) "Commercial" would mean for the purpose of promoting the sale, lease, or exchange of goods, services, or real property.

Do-Not-E-Mail List

The proposed Electronic Mail Solicitation Program would have to be administered by the DCIS or a program manager selected by the DCIS. The Program would have to be fully operational by January 1, 2004, or 90 days from the bill's effective date, whichever was later. The Program would have to maintain a list of e-mail addresses of people who did not want to receive unsolicited commercial e-mail.

A person could be included on the list by registering one or more e-mail addresses. The Program would be funded completely from the fees, fines, civil penalties, and forfeitures collected by the Attorney General for violations of the proposed Act. If the amount of funds collected for a fiscal year exceeded the Program's administrative cost, the excess amount would be deposited into the General Fund. A registration would be for a period of at least three years, at which point a person could renew the registration.

The Program would have to update the list at least every 30 days. It could not release to another person information concerning people or provide access to addresses on the list. The list would not be subject to the Freedom of Information Act and could not be sold or used for any purpose other than meeting the requirements of the proposed Act.

The DCIS, in consultation with the program manager, could create specific categories of e-mail for which recipients who were minors could receive protection. A parent, legal guardian, or other person with authority or control over e-mail addresses to which minors could have access, could list an e-mail address under any of the categories to give notice that he or she did not consent to receive e-mail within that category. The categories would have to include products or services that a minor is prohibited by law from purchasing. E-mail senders would have to honor the categories, even if they had evidence of a preexisting business relationship.

A listing in the registry would put all e-mail senders on notice that unsolicited commercial e-mail could not be sent to a name on the list unless the sender had a preexisting business relationship with the recipient. The notice would alert senders that they had to comply with all provisions of law and were subject to the State's jurisdiction when sending to addresses on the list.

Senders of commercial e-mail in Michigan would have to include a valid method to opt out of receiving future messages. A subscription to the registry and subsequent honoring of opt-out requests filed for the particular sender with the program manager would be considered an acceptable opt-out method.

A person who sent unsolicited commercial e-mail to an e-mail address in this State would have to register with the Program and pay an annual fee, as determined by the DCIS. A sender would be required to remove from its

mailing list addresses that appeared on the registry if the parties did not have a preexisting business relationship, if the type of mail the person planned to send were within one of the categories the recipient had opted out of, or if the e-mail holder had opted out of the specific sender's mailing list. A sender would have to update its list every 30 days with the latest available copy of the registry. If a person sent an unsolicited commercial e-mail without first verifying the recipient's e-mail address against the registry, the sending of the e-mail would be considered without the recipient's consent and would be a violation of the proposed Act. A registered sender would have to establish procedures to ensure that no unsolicited commercial e-mail was sent to a registered recipient. The burden of proof that the sender had the recipient's consent to send unsolicited commercial e-mail would be on the sender.

Required Information

A person who intentionally sent or caused to be sent an unsolicited commercial e-mail through an e-mail service provider that the sender knew or should have known was located in this State, or to an e-mail address that the sender knew or should have known was held by a resident of this State, would have to do all of the following:

-- Include in the e-mail a subject line containing "ADV:" as the first four characters.
-- Conspicuously state in the e-mail the sender's legal name, correct street address, valid internet domain name, and valid return e-mail address.
-- Conspicuously provide in the text of the e-mail, in print as large as the print used for the majority of the e-mail, a notice that informed the recipient that the recipient could conveniently and at no cost be excluded from future e-mail from the sender.

The sender also would have to establish a toll-free telephone number, a valid sender-operated return e-mail address, or another easy-to-use electronic method that the recipient could call or gain access to by e-mail or other electronic means, to notify the sender not to transmit any further unsolicited commercial e-mail messages. The notification process could include the ability for the recipient to direct the sender to transmit or not transmit particular e-mail based upon products, services, divisions, organizations, companies, or other selections of the recipient's choice. An unsolicited commercial e-mail would have to include, in print as large as the print used for the majority of the e-mail, a statement informing the recipient of a toll-free telephone number or valid return address the recipient could use to notify the sender not to transmit any further commercial e-mail messages.

Misrepresenting Information

A person who sent or caused to be sent an unsolicited commercial e-mail through an e-mail service provider located in Michigan or to an e-mail address held by a resident of Michigan would be prohibited from doing any of the following:

-- Using a third party's internet domain name or e-mail address in identifying the point of origin or in stating the transmission path of the e-mail without the third party's consent.
-- Misrepresenting any information in identifying the point of origin or the transmission path of the e-mail.
-- Failing to include in the e-mail the information necessary to identify its point of origin.

Additionally, a person could not knowingly sell, give, or otherwise distribute or possess with the intent to sell, give, or distribute software that was primarily designed or produced for the purpose of facilitating or enabling the falsification of e-mail transmission or routing information; had only limited commercially significant purpose or use other than to facilitate or enable the falsification of e-mail transmission information or other routing information; or was marketed by the person or another acting in concert with the person, with that person's knowledge, for use in facilitating or enabling the falsification of e-mail transmission information or other routing information. A person could not provide such software directly or indirectly to another person.

Sender Notification

A sender could not send unsolicited commercial e-mail, either directly or through a third party, to a recipient who notified the sender that he or she did not want to receive future e-mail. A sender would have to establish and maintain the necessary policies

and records to ensure that a recipient who notified the sender did not receive any e-mail from the date of the notice. The sender also would have to update its records at least every 14 business days.

The bill would allow an e-mail service provider to design its software so that a sender of unsolicited commercial e-mail would be notified of the requirements of the proposed Act each time the sender requested delivery of e-mail. The existence of the software would constitute actual notice to the sender of the Act's requirements.

An e-mail service provider that designed and implemented a dispute resolution process for a sender who believed the sender's e-mail message had been improperly blocked, and made contact information accessible on its website, would not be liable for blocking the receipt or transmission of the e-mail.

Penalties & Damages

A person who violated the proposed Act would be guilty of a misdemeanor punishable by imprisonment for up to one year or a fine of up to $10,000, or both. Each e-mail sent would be a separate violation. Additionally, all money and other income, including all proceeds earned but not yet received by a defendant from a third party as a result of the defendant's violations, and all computer equipment, software, and personal property used in connection with a violation that the owner knew was used in violation of the Act, would be subject to lawful seizure by a law enforcement officer and forfeiture by the State.

An action could be brought by a recipient of an e-mail sent in violation of the Act, an e-mail service provider through whose facilities an e-mail was transmitted in violation of the Act, or by the Attorney General. In each action, a recipient, an e-mail service provider, or the Attorney General could recover either actual damages or the lesser of the following: $500 per unsolicited commercial e-mail, or $250,000 for each day the violation occurred. Additionally, a prevailing recipient or e-mail service provider would have to be awarded actual costs and reasonable attorney fees.

The bill states that an e-mail service provider would not be in violation of the Act solely by being an intermediary between the sender and recipient. Also it would be a defense to any criminal or civil action that the unsolicited commercial e-mail was sent accidentally. The burden of proving accidental transmission would be on the sender.

BACKGROUND

Several other states have enacted anti-spam legislation. The first was Nevada, which began in 1997 to require marketers to offer recipients a way to be removed from e-mail lists. Washington prohibits sending e-mails with false or misleading subject lines or sender information. Several states require unsolicited e-mail to be identified with the letters "ADV" in the subject line, and some allow recipients to sue the sender and seek monetary damages.

In April 2003, Virginia enacted the nation's toughest anti-spam law to target people who send fraudulent, bulk e-mail. Under the new law, it is illegal to forge the return address line or hack a computer to send spam without the owner's knowledge, and those found guilty of sending more than 10,000 such deceptive messages are subject to imprisonment for up to five years and forfeiture of profits and assets connected with the activities. No state has a state-administered registry.

The European Union (EU) has instituted rules to combat spam, most of which originates in the United States. In Italy, repeat offenders are fined an average of $280, and in Spain, spammers can be fined more than $34,000. The EU nations are expected to implement "opt-in" policies, under which an e-mail marketer could send e-mail only to people who requested it, by the end of this year.

Spam also is the subject of scrutiny at the Federal level. The Federal Trade Commission recently conducted a three-day forum on spam, and several bills have been introduced in both houses of Congress. These proposals include the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM, S. 877), the Restrict and Eliminate Delivery of Unsolicited Commercial E-mail Act (REDUCE, H.R. 1933), and the Reduction in Distribution of Spam Act (RID Spam, H.R. 2214). All would require unsolicited commercial e-mail to be clearly labeled as advertising and contain a valid return e-mail address at which the recipient could notify the sender that he or she did not want to receive future e-mails. Additionally, including false or misleading material in the

subject line or point of origin would be prohibited. Penalties for violating the proposed Acts would include fines and prison time, and a recipient, ISP, or state attorney general could bring a civil action against a violator. The RID Spam Act would allow the United States Attorney General to bring a civil action, as well, and specify that anyone who sent at least 10,000 e-mails in a 30-day period would be subject to the penalties of the Act. Both the CAN-SPAM Act and the RID Spam Act would prohibit a spammer from obtaining e-mail addresses from the internet through automated means, or "harvesting". The REDUCE Spam Act would set up a bounty system for the first person to report a particular spammer.

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

Some say that spam threatens the future of one of the greatest technological advances in recent times. What began as a minor nuisance has become a costly obstacle for the business community and an invasion of privacy in the home. Due to the onslaught of spam, some people have chosen to abandon e-mail and return to more conventional means of communicating. Reportedly, in Japan, many people are canceling their cell phone services and using traditional telephones because 90% of text messages are now spam. It is ruining e-mail as a fast, effective communication tool, something that could have serious economic repercussions.

The cost of spam in the United States already is astronomical, and will continue to rise as spam increases exponentially. According to Senate Committee testimony, the cost to businesses in lost productivity will be $10 billion in 2003, and will likely reach $75 billion by 2007 if something is not done. The cost to Michigan businesses in 2003 will be $350 million. Businesses also will spend $653 million nationally in 2003 on e-mail filters, a cost that is expected to rise to $2.4 billion by 2007. These figures do not include the money businesses must spend on technicians to repair system crashes or fix the damage done by viruses originating in spam.

Spam also facilitates on-line fraud. The Federal Trade Commission recently announced that two-thirds of unsolicited bulk e-mails contain misleading or deceptive information. Among e-mails containing information about investment and business opportunities, an estimated 96% are false or misleading. In 2002, Michigan residents lost $21 million due to on-line fraud, much of that as a result of deceptive spam. Additionally, internet customers must pay higher rates for increased bandwidth and the cost of processing the barrage of e-mails flooding the network. Bulk e-mail can contribute to slower internet connections.

While businesses and residents have collectively lost billions of dollars due to spam, it costs spammers very little to send the messages. They can purchase a list of 10 million e-mail addresses for $1,200 and, operating on several computers in their basements, can send millions of e-mails in a matter of hours. Spammers often see the fines that currently can be imposed upon them as a cost of doing business, thereby hindering the effectiveness of current laws in curtailing spam. The bill would provide an arena in which to prosecute them and the prescribed penalties could significantly increase their cost of business.

Supporting Argument

While laws regulating unsolicited commercial e-mail have been passed in other states, they have been largely ineffective because they do not establish a "nexus" that gives the state jurisdiction over the people sending spam. By creating a registry within the DCIS, the bill would establish this nexus, which is crucial in prosecuting spammers. Some states that have passed anti-spam laws have been plagued by the problem of enforceability and are now considering a do-not-spam registry. The registry would eliminate a spammer's claim that it is impossible to know which state's laws apply to which e-mail addresses, and would put Michigan in a better position than other states to combat spam. Under the bill, it would be clear whether someone had violated the law, and it would be relatively easy to bring a civil or criminal action against a spammer. Although the bill would not stop spam entirely, it would go further in the right direction than other states' attempts and provide another tool in a multipronged attack against spam.

Response: If anti-spam legislation is enacted, it should be at the Federal level

rather than the state level. Legitimate companies trying to market their products could be impeded by a patchwork of state laws, and companies with a presence in several states could face multiple liabilities.

Supporting Argument

According to Committee testimony, as much as 30% of unsolicited e-mail is generated by "adult" websites. This makes parents very concerned about their children's receiving spam. In addition, spam presents a unique problem for businesses because an employee inadvertently could open an e-mail containing inappropriate or adult content, thereby subjecting the employee and the company to claims of creating a hostile work environment and sexual harassment. Under the bill, businesses could register their employees' e-mail addresses, and parents could register their children's, to filter out pornographic material.

Opposing Argument

It is possible that the bill would not significantly reduce the amount of spam people receive, and it certainly would not halt the flow altogether. One reason that spammers have been successful in evading the consequences of their actions is that it is easy for a person to conceal his or her identity in sending an e-mail. A person could choose to ignore the law by failing to provide the required contact information and continue sending millions of unwanted e-mails every day. An overseas spammer probably would not be deterred by a Michigan law, as the likelihood of someone identifying him or her and then following through with a court case is small. The bill could encourage spammers to go overseas, out of the reach of the legal system.

Response: No legislation can completely stop spam, but the bill would provide an opportunity for recourse for the millions of people who feel annoyed or harassed every day, and the businesses that are losing money. Even if the bill resulted only in a reduction of spam, it would provide a valuable service to Michigan residents.

Opposing Argument

There is debate over the definition of "spam", and the bill does not offer a definition, either. In the course of the Committee testimony, several people made the distinction between "spammers" and "legitimate marketers", saying that spam is generally deceptive. Many people, however, probably consider all unsolicited e-mail an annoyance, whether or not it is deceptive. Even internet service providers send commercial e-mails, sometimes millions every day, to their customers. While the messages do not contain false information and the origin is not hidden, many people would consider these e-mails spam that they would like to avoid. Under the bill, as long as e-mail marketers adhered to certain practices, they could continue to send their unwanted e-mails to millions of people.

Opposing Argument

The bill would unfairly put the burden on recipients to register with the DCIS. An "opt-in" method would be more appropriate than the "opt-out" method in the bill. People should receive spam only if they have a preexisting business relationship with the marketer or specifically request to receive it. Since every legitimate e-mail marketer already uses an "opt-in" method, the bill would set a lower standard than the one the industry has already. According to Committee testimony, several state and national governments that have enacted "opt-out" laws have found them to be ineffective and are considering "opt-in" laws.

Response: The point of advertising is to introduce people to new products and services. People cannot "opt in" for something of which they are unaware. Some people actually buy the products or services advertised in e-mail that they did not ask to receive. E-mail is not spam merely because it is unsolicited. Bulk e-mail is simply a marketing tool, just like any other advertising method that businesses use to increase exposure to their products.

Opposing Argument

Society should rely more on the internet industry and less on government to solve the problem of spam. Competition will force internet service providers to continue improving their filtering software, making it more attractive to potential customers. The underlying premise of the internet is that it is free from regulation, its development driven by the people who use it. The entities with the most stake in the issue, the internet companies, will find the most efficient way to control the flow of spam because they must do so in order for their businesses to survive.

In addition to increasingly sophisticated filtering technology, some ISPs have suggested a self-regulatory approach, in which ISPs would provide commercial senders with a seal of approval for following a set of best

practices, such as labeling their messages as advertisements and providing valid return e-mail addresses. Legitimate marketers would be willing to comply in order to protect their business interests, while deceptive spammers would be more easily filtered out. Using this method, just as several volunteer groups have posted "blacklists" of alleged spammers, ISPs would "whitelist" those marketers who were not deceptive or fraudulent.

Opposing Argument

The bill would violate a sender's constitutional right to free speech and a recipient's right to see his or her e-mail. People already have the option of deleting unwanted e-mail or installing filtering software on their computers.

Response: While a person might have a right to send e-mail, commercial speech does not fall under the same protection that personal speech does. Individuals and businesses also have the right to regulate what comes into their homes or workplaces, and reject material they do not want. A spammer should not be allowed to invade the privacy of others by sending uninvited pornography or other inappropriate material to unsuspecting families and employees. Furthermore, as filtering software becomes more sophisticated, spammers continue to find ways to evade it. As a result, not only do people continue to receive spam, but messages that are not spam are blocked.

Opposing Argument

A do-not-e-mail registry raises concerns about privacy and unintended consequences. Perhaps the most obvious concern is that an unscrupulous person could obtain the list and use it to bombard the people on it with unwanted e-mails. Currently, the job of eliminating the e-mail addresses of people who do not want to receive unsolicited e-mail falls on the sender; under the bill, the State would take over this job, which could result in the transmission of even more spam to people who were not on the list.

There are ways to go after spammers without jeopardizing privacy, such as prosecuting under existing fraud statutes. For example, a man known as the "Buffalo Spammer" was charged with forgery and identity theft in connection with the 825 million spam e-mails he sent in the last year. He allegedly replaced his own e-mail address with those of other people to hide the origin of the e-mails and used stolen credit card numbers to sign up for 343 internet accounts from EarthLink, to which he was ordered to pay $16.4 million after failing to respond to a civil suit the company had brought against him in Federal court.

In another case, a man pleaded guilty to a Federal misdemeanor charge of damage to a protected computer system after he sent more than 500,000 angry e-mails to Boston Fox affiliate WFXT-TV 25 because the station broadcast a Red Sox game instead of a NASCAR race.

Response: The registry could be encrypted so that people would not have to worry about the misuse of their personal information. According to a representative of Unspam.com, the company is developing software that would take a hacker 5,000 years to crack. Additionally, the bill specifically states that the list could not be used for any purpose other than the purpose of the proposed Act, and would prohibit the information on the list from being shared. The registry also would not be subject to the Freedom of Information Act. While several spammers have been prosecuted under existing laws, there have not been many successful prosecutions, and they have not led to a decrease in the flow of spam.

Legislative Analyst: Julie Koval

FISCAL IMPACT

Revenue to the Program would depend on the number of unsolicited commercial e-mail senders that registered. Enforcement costs would depend on the number of violations. The Department of Consumer and Industry Services does not have an estimate regarding its administrative costs.

There are no data to indicate how many offenders would be convicted of violating the proposed Act. Local units of government would incur the costs of misdemeanor probation and incarceration in a local facility, which varies by county. Public libraries would benefit from any additional penal fine revenue collected.

Fiscal Analyst: Maria Tyszkiewicz
Bethany Wicksall

A0304\s357b