House
Legislative
Analysis
Section

House Office Building, 9 South
Lansing, Michigan 48909
Phone: 517/373-6466

REGULATE UNSOLICITED COMMERCIAL EMAIL

House Bill 4519 as enrolled
Public Act 42 of 2003
Second Analysis (7-14-03)

Sponsor: Rep. Bill Huizenga
House Committee: Energy and Technology
Senate Committee: Technology and Energy

THE APPARENT PROBLEM:

Advertisers have long claimed that their right to free speech allows them to provide potential customers with information about goods and services. Consumer advocates often reply that respect for individuals' right to privacy demands acknowledging that certain spheres of person's lives should be free from the uninvited and unwelcome intrusion of others. Reality is of course more complex, as advertisers rarely confine themselves to providing comprehensive, balanced information about their wares, and despite their protests to the contrary, people are often happy to learn about unfamiliar goods and services, regardless of whether the messenger has a financial stake in the interaction. The regulation of unsolicited direct mail advertising, telephone solicitation, and more recently unsolicited commercial e-mail is an attempt by governments to find a nuanced middle ground.

"Spamming" is the mass distribution of unsolicited electronic mail (e-mail) messages, whether for commercial or noncommercial purposes. The e-mail messages themselves are called "spam". While mass distributed unsolicited e-mail need not be sent for commercial purposes, and there is no reason why unsolicited commercial e-mail (UCE), like direct mail advertisements and telephone solicitations, cannot be tailored to individuals, spamming is generally valued and reviled as an inexpensive way for advertisers to promote goods and services to large numbers of people. Inexpensive for the sender, that is: e-mail ads do not involve the paper and postal costs of direct mail advertising, and the personnel and phone costs are far less than those for telemarketing sales.

To understand why spamming is such an attractive technique for many advertisers and such an aggravating nuisance for many e-mail users, it helps to understand more about the practice itself.

There are two basic ways that advertisers go about spamming: advertisers may send a single message--or a message whose content varies slightly--to multiple Usenet newsgroups or they may send a single message to multiple e-mail addresses. Advertisers send e-mails to newsgroups primarily to target "lurkers" who read a group or groups' messages, but do not subscribe to groups or share their e-mail addresses publicly. Though the primary target of the spam may be the lurkers, newsgroups have reportedly broken up when participants have become frustrated by the dwindling number of posted messages that have anything to do with the newsgroup's purported subject matter.

Alternatively, or in conjunction with newsgroup spamming, advertisers may mass distribute messages to e-mail addresses. In some cases, these addresses are obtained when businesses ask for permission to notify their customers about the availability of new products, discounts, and other items of interest by e-mail. Yet a report by the Center for Democracy and Technology suggests that most businesses that have an ongoing relationship with a customer generally respect customers' express wishes not to receive e-mail ads. The real problem for consumers appears to be businesses and marketers that gather or guess e-mail addresses of the public at large and figure that they stand to gain if they receive even a handful of replies after spamming thousands, hundreds of thousands, even millions of e-mail addresses. Addresses may be found by "mailbots" that "sweep" or "scrape" the Internet for unbroken character strings that use the "@" symbol, judging that the majority of them will be valid e-mail addresses. Alternatively, "brute force" and "dictionary" programs "think up" plausible user names (e.g.,

"johndoe", "marysmith", and "abc123"), and attach them to an @ symbol followed by one or more popular domain names (e.g., Internetserviceprovider.com, nonprofitentity.org, and college.edu) allowing spammers to send messages to addresses that seem likely--but are not known--to be occupied. Regardless of how one gets on a spammer's mailing list, removing oneself from the list may be very difficult. Spammers often fail to leave any valid contact information, and even if they do, they may ignore requests to be removed from the list or, worse yet, take any response whatsoever as a sign that the address is occupied, and therefore, ripe for future spamming.

Further, as noted above, spam is cheap for the sender. One of the reasons that commercial spam has provoked so much indignation among recipients is that it shifts the cost burden of advertising from the marketer--or ultimately the *actual* customer who buys the good or service at a price that reflects the advertising cost--to the *potential* customer. Generally speaking, the spammer incurs only the costs of personnel for writing and sending the message, obtaining e-mail addresses and an Internet connection. In an April 2003 article *The Economist* reports that CDs can be bought for $5 per million addresses, and whatever the other costs are, they are fairly negligible when divided by 100,000 or 1,000,000 recipients. According to committee testimony (and corroborated by newspaper and magazine articles, letters to the editor, and information provided by anti-spam groups) it is not unusual for people to come into work on a Monday morning to find 100 or more spam messages or to come back from lunch to find a dozen spams sitting in their in-boxes. Opening and deleting the messages means lost productivity to their employers.

Then, when people leave work for the day and go home and check their personal e-mail accounts, they may find several more spams awaiting them. Opening and deleting those messages deprives recipients of their own time and possibly money, if for example they have a dial-up connection and pay phone charges by the minute or have a restricted number of "free" minutes through their Internet service provider. While some people learn to recognize spam fairly quickly, an employee may be very hesitant to delete a message until she is absolutely sure it has nothing to do with her work, and people who post messages to the web frequently may be used to receiving e-mails from people they do not know. People who do not use e-mail frequently may have a more difficult time distinguishing between legitimate e-mail solicitations and abusive or fraudulent offers. The nuances of individuals' e-mail habits may make it difficult to determine the precise costs of spam in time and money to businesses and ordinary e-mail users, but it is clear that the costs can be significant.

Then, there are other, less tangible costs of spam: consider the employee or child who receives a message containing pornography. Regardless of one's web browsing history, anyone can receive such messages, and this may in turn lead a supervisor or parent to suspect that their employees and children have been seeking such inappropriate content. This can create tension in the home or workplace, which may not be easily quantifiable.

The scope of the problem is huge. *The Economist* cites one estimate that spam accounts for 45 percent of all e-mail traffic. In addition, the article reports that America Online (AOL) "blocks an average of 780 million junk e-mails daily, or about 100 million more e-mails than it actually delivers"! AOL and other e-mail address providers offer their address holders the option of having spam--or rather, e-mail that appears to be unsolicited and unwanted--sent to a junk mail folder. Those who choose this option can adjust the settings so that the folder purges itself on a daily or other periodic basis. Others have independently composed "black lists" outing spammers. Filtering invariably leaves gaps, letting some UCE through, and blocks some wanted e-mail from reaching addressees. Moreover, filtering e-mails is time-consuming and expensive, whether it is an individual e-mail address holder trying to sort through the wanted and junk e-mail messages or an e-mail address provider trying to keep address holders happy by preventing the junk from ever reaching their in-boxes. And black lists leave judgments about who is a spammer and who is not to the discretion of whoever creates the lists. Being misidentified as a spammer can create problems for "legitimate" e-mail senders, while illegitimate senders often "hijack" e-mail addresses and domain names to spam, creating difficulties for the victimized e-mail address or domain name holder who must then explain that he is not the spammer.

AOL has joined forces with major competitors Microsoft and Yahoo to collectively target the problem, and in late April and early May, the Federal Trade Commission held a three-day conference addressing spam. Various federal legislative proposals have been introduced and debated, and over half the states have enacted their own anti-spam legislation. Many people believe that Michigan should do the same.

THE CONTENT OF THE BILL:

The bill would create a new act, the "Unsolicited Commercial E-mail Protection Act", to regulate e-mail messages that promote goods, services, real property, and other things of value and are sent without the recipient's express permission. Senders of unsolicited commercial e-mail messages (UCE) would have to identify themselves, indicate in the subject heading that the message contained an advertisement, and allow recipients of such ads to "conveniently and at no cost" opt out of receiving future UCE from the sender. In addition, the bill would prohibit the falsification or misrepresentation of a message's point of origin or transmission path and would prohibit knowingly selling, giving, or otherwise distributing software that falsifies such information. Finally, the bill would provide criminal penalties for such violations and establish a cause of civil action allowing recipients, service providers, and the attorney general to recover damages for violations. If enacted, the bill would take effect on September 1, 2003. A detailed summary of the bill's provisions is provided below.

Identification of sender/nature of message and opt-out provisions. A person who intentionally sent or caused to be sent an unsolicited commercial e-mail message through an e-mail service provider that the sender knew or "should have known" was located in Michigan or to an e-mail address that the sender knew or "should have known" was held by a Michigan resident would have to do both of the following:

- include in the e-mail subject line "ADV:" as the first four characters;

- and conspicuously state in the text of the e-mail the sender's name, correct street address, valid Internet domain name, and valid return e-mail address.

The sender (or person who caused the message to be sent) would also 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 of the commercial e-mail could use to notify the sender not to send anymore UCE. The notification process could include notification of the recipient's ability to direct the sender to transmit or not transmit particular commercial e-mail messages based upon products, services, divisions, organizations, companies, or other selections of the recipient's choice. Also UCE would have to include, in print as large as the print used for the majority of the message, a statement informing the recipient of a toll-free number that the recipient could call, or a valid return address to which a recipient could write or access by e-mail, notifying the sender not to send any further commercial e-mail messages. Finally, the sender would have to 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 UCE from the sender, as provided above.

"Commercial e-mail" would be defined as an electronic message, file, data, or other information promoting the sale, lease, or exchange of goods, services, real property or any other thing of value that was transmitted between two or more computers, computer networks, or electronic terminals within a computer network. An e-mail would be considered "unsolicited" if it was sent without the recipient's express permission, unless the sender had a preexisting business or personal relationship with the recipient, or the e-mail was received as a result of the recipient opting into a system in order to receive promotional material. A "preexisting business relationship" would be defined as a relationship existing before the receipt of an e-mail formed voluntarily by the recipient with another person by means of an inquiry, application, purchase, or use of a product or service of the person sending the e-mail.

Disclosure of transmission/routing information. A person who sent (or caused to be sent) UCE through an e-mail service provider located in Michigan or to an e-mail address held by a resident of Michigan could not do any of the following: use 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 ad without the third party's consent; misrepresent any information in identifying the e-mail's point of origin or the transmission path; fail to include the information necessary to identify the e-mail's point of origin; or provide (directly or indirectly) another person with software prohibited under the act (see below).

Notification to stop sending unsolicited ads. If the recipient of UCE notified the sender that he or she did not want to receive future UCE from the sender, the sender could no longer send UCE to the recipient directly or through a subsidiary or affiliate. Senders of UCE would have to establish and maintain the necessary policies and records to ensure that such recipients did not receive e-mail from the date of the

notice, and would have to update their records at least once every 14 business days.

Sale or distribution of software to falsify transmission/routing information. A person could not knowingly sell, give, or otherwise distribute, or possess with the intent to sell, give, or distribute software that did any of the following: was primarily designed or produced for the purpose of facilitating or enabling the falsification of commercial e-mail transmission information or other routing information; had only "limited commercially significant purpose or use" other than facilitating or enabling the falsification of such information; or was marketed by the person or another acting in concert with that person with that person's knowledge for use in facilitating or enabling the falsification of such information.

Service provider's ability to design software to give notice of act's requirements. An e-mail service provider could design its software so that a sender of UCE is given notice of the requirements of the (proposed) act each time the sender requests delivery of e-mail. The existence of such software would constitute actual notice to the sender of the act's requirements. An e-mail service provider that designs and implements a dispute resolution process for a sender who believes the sender's e-mail message has been improperly blocked, and makes contact information available on its web site, would not be liable for blocking the receipt or transmission of the e-mail.

Penalties. In general, a violation of the act would be considered a misdemeanor punishable by up to one year of imprisonment and a fine of up to $10,000. However, persons who violated prohibitions relating to the disclosure of routing and transmission information described above and persons who violated the act in the furtherance of another crime would be guilty of a felony punishable by up to four years in prison and a fine of up to $25,000. Each commercial e-mail sent in violation of the act would be a separate violation.

An e-mail service provider would not be considered to have violated the act as a result of being an intermediary between the sender and recipient of UCE that violated the act. Nor would an e-mail service provider be considered to have violated the act by providing transmission of UCE over its network or facilities.

It would be prima facie evidence that a sender was in violation of the section of the bill setting forth the criminal penalties for violations of the act if the recipient was unable to contact the sender through the return e-mail address provided by the sender.

Remedies. A civil suit against the sender of UCE sent in violation of the act could be brought by any of the following: a person who received UCE in violation of the act; an e-mail service provider through whose facilities the UCE was transmitted; and the attorney general. In each such action, a recipient, the service provider, or the attorney general could recover actual damages or, in lieu of actual damages, the lesser of either $500 per UCE received or transmitted or $250,000 for each day the violation occurred. The prevailing recipient or service provider would be awarded actual costs and reasonable attorney fees.

UCE sent accidentally or as a result of a preexisting business relationship. It would be a defense to a criminal or civil case brought for a violation of the act that the UCE was transmitted accidentally or as a result of a preexisting business relationship; the sender would have the burden of proving that the UCE was transmitted accidentally or as a result of a preexisting business relationship.

BACKGROUND INFORMATION:

"spam", not "SPAM". Hormel Foods, producer of the SPAM family of meat products, which it touts as (possibly) the "fastest-growing segment of the human imagination since the sweater-vest was invented", neither engages in the mass distribution of unsolicited commercial e-mail nor objects to the use of the term "spam" to describe the unsavory practice. The company does object to the use of images of its products in association with UCE, however, and suggests that when using the term in lieu of "mass-distributed, unsolicited e-mail" writers use lower-case letters.

Happily, for etymology buffs and SPAM-aficionados alike, the connection between "spam" and "SPAM" is not entirely fortuitous. Commentators agree that the use of the term "spam" to refer to mass e-mailing has its origins in a skit by Monty Python, the famous British-comedy troupe, in which a waitress describing her restaurant's culinary offerings to a horde of Vikings repeats "SPAM" several times to emphasize just how much of the canned spiced ham product they contain. The Norsemen respond by singing the term "SPAM" repeatedly and ever more loudly, until they drown out other conversation and are then told to be quiet. By analogy, opponents of mass e-mailing suggest that spam clogs up in-boxes

and prevents e-mail users from effectively communicating with others who they would like to send messages to and receive messages from.

FISCAL IMPLICATIONS:

There is no fiscal information at present.

ARGUMENTS:

For:

In the words of Lawrence Lessig, a law professor known for his expertise on Internet issues, "Spammers say there are lots of people out there who love to receive spam. Good for them. They can tell their [i]nternet service provider or e-mail client to deliver all e-mail, regardless of the subject line. But those of us who actually work for a living can choose to ignore this class of junk on the Internet by filtering all e-mail with the subject line [ADV:]". While Lessig's choice of words may be a bit harsh, the sentiment behind the words reflects the opinion of many people that if they must receive some unsolicited commercial e-mail (UCE), they should have a clear warning of what is contained in the message, so they can choose whether to delete the message instantly or peruse its contents. The bill would not prohibit UCE but rather would require senders to let recipients know the nature of the message and to give consumers various options to express preferences for future solicitations, including receiving none at all.

UCE threatens people's fair use of the Internet by clogging up in-boxes and littering newsgroups with irrelevant postings. The estimates of the amount of UCE sent each day are staggering and if the matter is left unaddressed the problem will only get worse. Many opponents of UCE stress that they have no gripes with legitimate business activity. Because it is so cheap for the sender, however, spamming allows virtually anyone with an Internet connection to tout goods and services to a worldwide audience, leaving recipients with the job of dealing with it. Legitimate businesses understand why individuals and businesses who receive UCE resent having to bear the costs of UCE. While spammers argue that they are just giving a new twist to direct advertising and that the low cost of business removes barriers to entry to the marketplace, very few legitimate business use unsolicited commercial e-mail (UCE) and those that do generally respect recipients' wishes to be removed from mailing lists to avoid alienating their customer base. According to the Coalition Against Unsolicited Commercial E-mail, most UCE consists of chain letters, "pyramid" and other "get rich quick" schemes, phone sex solicitations and other ads with pornographic content, offers of "quack" health products and dubious home remedies, illegally pirated software, and other illegitimate offers. Recognizing that legitimate businesses have an interest in contacting potential customers, the bill wisely allows businesses to contact individuals they have preexisting business relationships with and individuals who have given them their e-mail addresses.

The bill includes several other provisions which will help address the spam problem comprehensively. For instance, the bill explicitly prohibits UCE senders from misrepresenting their messages' point of origin or transmission path and prohibits the sale, gift, or distribution of software designed to falsify such information. Also, the bill would allow e-mail service providers to automatically notify UCE senders of the bill's requirements. Such requirements should assist those bringing suits under the bill by helping them to establish that abusive spammers took steps to avoid being identified as the sender of UCE and that they knew the law they were violating.

Response:

Many people who dislike UCE support efforts to restrict it or eliminate it altogether but question whether state legislation is the right solution. Spam accounts for millions, perhaps even billions, of the e-mail messages that are sent each day. Many of these messages are sent from other states and other countries, and tracking spammers down and getting them in court would be a daunting task. While over half the states have anti-spam legislation on their books, this creates a confusing patchwork of laws for legitimate businesses who want to play by the rules. Rather than adding to the confusion, Michigan should join with other states to enact federal legislation. Ultimately, achieving a solution to the problem may require international cooperation since e-mail messages basically ignore national boundaries.

Others believe that UCE should be prohibited altogether. If people want to receive offers from businesses, they should certainly be allowed to request that they be sent by e-mail, but individuals—particularly who pay for their e-mail accounts and Internet access—should be allowed to use their accounts the way they choose and should not have to put up with unwanted commercial solicitations.

Reply:

While federal legislation or a uniform framework of state laws may be ideal, the bill represents an important first step in tackling the spam problem and urging Congress to act. While enforcement is not necessarily going to be easy, the bill would give the state some valuable tools to go after spammers.

The point of the legislation should not be to stifle legitimate commercial activity. Businesses should be allowed to alert consumers to the virtues of their goods and services as long as they agree to follow individual consumers' wishes about future solicitations. Requiring consumers to "opt in" would hurt new businesses as well as existing businesses that have developed goods and services that people do not know about.

Against:

Unapologetic in her defense of UCE, e-mail marketer Alex Sachs was quoted in an April *New York Times* article as stating that " '[t]hese antispammers should get a life' . . . . 'Do their fingers hurt too much from pressing the delete key? How much time does that really take from their day?' ". Sachs suggests that "antispammers" do a great disservice to the millions of people with bad credit (among others) who would miss out on credit-related offers if those who oppose UCE have their way.

Direct mail advertising, telephone solicitation, and e-mail messages are effective and legitimate means of marketing goods and services. Businesses do in fact use these techniques, and if they did not work, businesses would find more effective ways to market their products. Because they work, some of those who received the solicitations must be happy to have done so, regardless of what they say about so-called "junk" mail, telemarketing calls, and "spam" when asked by pollsters. Besides, advertising is protected as free speech in this state and country, and legitimate businesses should be free to e-mail potential customers, whether or not UCE works. Consumers enjoy the power of the purse, and advertisers and other businesses who acquire a reputation for abusive and harassing practices will alienate their customer base and go out of business.

While it may seem fair to require marketers to warn people of a message's content with the characters "ADV:" and to allow them to opt out of future offers from individual businesses, this will only hurt legitimate businesses, which will obey the requirements, and will not affect the practices of the illegitimate spammers who everyone agrees are the real source of the problem.

Analyst: J. Caver

■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.