PRB 03-37E

THE SPAM SCOURGE

Lalita Acharya
Science and Technology Division

10 February 2004

PARLIAMENTARY RESEARCH BRANCH
DIRECTION DE LA RECHERCHE PARLEMENTAIRE

The Parliamentary Research Branch of the Library of Parliament works exclusively for Parliament, conducting research and providing information for Committees and Members of the Senate and the House of Commons. This service is extended without partisan bias in such forms as Reports, Background Papers and Issue Reviews. Analysts in the Branch are also available for personal consultation in their respective fields of expertise.

CE DOCUMENT EST AUSSI PUBLIÉ EN FRANÇAIS

TABLE OF CONTENTS

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

THE SPAM SCOURGE

INTRODUCTION

The Internet and electronic mail (or "e-mail") have revolutionized the way many of the world's citizens live and do business. In recent years, however, an increasing volume of unsolicited and unwanted e-mail, commonly referred to as "spam," has compromised the benefits of e-mail and undermined consumer confidence in electronic communications. This paper examines why spam is a problem and what technological, legal and other approaches are being employed to deal with it around the world. The situation in Canada is discussed, as is the debate about the need for legislation in Canada to control spam.

WHAT IS SPAM AND HOW MUCH IS SENT EACH YEAR?

There is no universally accepted definition of spam. Some commentators limit the term to unsolicited, bulk e-mail(1) or unsolicited, commercial e-mail, whereas others include any unsolicited e-mail. A broader definition of spam includes any unsolicited electronic messaging, regardless of its content, the size of the mailing or the nature of the communications medium.(2) The percentage of e-mail that is spam(3) has ballooned over the last few years, growing from 7% in April 2001 to 60% in January 2004.(4) One anti-spam software company has predicted that the percentage of e-mail that is classified as spam will increase to more than 75% in 2004.(5)

---

(1) See, for example, the Spamhaus Project, http://www.spamhaus.org/definition.html.

(2) See, for example, Government of Australia, National Office for the Information Economy, *SPAM: Final Report of the NOIE, Review of the Spam Problem and How It Can Be Countered*, April 2003, p. 7, http://www.noie.gov.au/publications/NOIE/spam/final_report/SPAMreport.pdf.

(3) Unless specified otherwise, the word "spam" in this paper refers to unsolicited e-mail.

(4) Brightmail, Spam Statistics, http://www.brightmail.com/spamstats.html.

(5) Postini, Inc., "Incidence of spam, viruses, and fraudulent email attacks to increase dramatically in 2004," December 2003, http://www.postini.com/press/pr/pr121703.html.

Spam may contain information on legitimate or illegitimate products and services, including advertisements for general merchandise, financial services, health products and services, pornography, computer software and educational services. Spam is also used to send political and religious messages.

WHY IS SPAM A PROBLEM?

A. Message Content and Ethical/Criminal Considerations

At a fundamental level, many e-mail recipients object to receiving unsolicited e-mail because dealing with it is annoying and time-consuming, regardless of its content or intent. Other individuals object to spam because its content is often deceptive, fraudulent or considered offensive by the recipient. According to some estimates, approximately 18% of spam is advertisements for adult entertainment products or services.(6) Because spammers do not usually target their audience, children are frequently the recipients of spam.

There are numerous examples of deceptive spam that offers phoney get-rich-quick schemes and prizes.(7) A relatively new spam problem, known as "phishing," involves the theft of sensitive personal information. Spammers who are phishing send e-mails that appear to come from legitimate companies. The e-mails direct the recipients to visit a Web site (by clicking on an embedded URL) where they are asked to update personal information (e.g., passwords and credit card numbers) that the legitimate organization already possesses. The Web site, however, is bogus and set up only to steal the recipients' personal information.(8)

B. Financial Cost

In most forms of communication (e.g., sending flyers by the post), there are significant costs for the sender, so the sender balances the expected benefits of the communication against the costs. Accordingly, the sender must make decisions about how widespread the information or advertising campaign will be in an attempt to spend resources

---

(6) Brightmail, Spam Categories, http://www.brightmail.com/spamstats.html.

(7) For examples of deceptive spam schemes, see the case chart on the Spam e-mail page of the U.S. Federal Trade Commission's Web site, http://www.ftc.gov/os/2003/05/swnetforcepresschart.pdf.

(8) See Anti-phishing.org for further information, http://www.antiphishing.org.

efficiently. With spamming, however, the sender spends very little money to send messages, and the size of the mailing can thus be much larger than via more conventional modes of communication. The costs of dealing with spam are instead borne by the Internet Service Provider (ISP) and the e-mail recipient. Although the information contained in some spam may be useful to some of its recipients, most of it is unwanted and is filtered or deleted by the e-mail recipient or by the ISP.

As the volume of spam has increased in recent years, so have the financial costs of dealing with it. A 2001 European study estimated that the connection costs for global Web surfers just to download spam using the mostly widely available technology was approximately €10 billion (or approximately CAN$16.8 billion) a year.(9) Customers may also end up paying a higher rate for Internet access because of spam. Service providers pay for bandwidth based on anticipated use by the client base. When a spammer begins to use an ISP's bandwidth, the ISP's clients suffer slower Internet access. If the ISP wishes to increase the speed of access, the ISP must either buy increased bandwidth, or invest in systems to block or filter the spam. In either case, the costs of dealing with spam are usually passed on to the ISP's customers.

Dealing with spam is also costly for businesses. Unless a company has a service to filter or block spam (services that are not 100% effective anyway), employees may spend a relatively large amount of time deleting spam from their accounts. Although the time spent dealing with spam may be only seconds a message, productivity losses to the company accumulate over time. A recent report estimated that spam is costing corporations globally approximately US$20 billion (or CAN$27 billion) annually in terms of information technology (IT) spending (e.g., for increased bandwidth, storage costs, anti-spam software and user support) and lost productivity, and that the cost is growing by almost 100% a year.(10)

---

(9) Serge Gauthronet and Etienne Drouard, *Unsolicited Commercial Communications and Data Protection*, Commission of the European Communities, January 2001, http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamstudy_en.pdf.

(10) The author of the study does not provide any information as to how this figure was estimated. See Jonathan B. Spira, *Spam E-Mail and Its Impact on IT Spending and Productivity*, Basex, December 2003, http://www.basex.com/poty2003.nsf/e67dc0f5617d6e9c85256a99005ea0e7/f8761f74ba37069385256e040019f314/$FILE/BasexReport.Spam.pdf.

C. Displacement of Other E-mail and "Blended Threats"

In addition to the financial cost of dealing with spam, spam also poses a threat to the reliability and security of Internet communications. Spam can flood e-mail servers, reducing or preventing the passage of legitimate e-mail traffic. A newer spam problem involves "blended threats," or the bundling of viruses, worms or Trojan horses with spam. In 2003, for example, a mass-mailing worm known as Sobig.C spread copies of itself through e-mail messages bearing attached files that contained the virus code. Sobig.C's replication was likely enhanced by spam technology to achieve greater spreading speed and global distribution.(11)

HOW DO SPAMMERS OPERATE?

Sending spam is an extremely cheap and quick method for companies and individuals to send advertisements for products and services or other types of information to anywhere from a few individuals to a few million individuals. Spammers need only have access to the appropriate software tools, or "spamware," to start sending unsolicited messages either directly through their personal ISP accounts or anonymously via third-party "open relay"(12) or "open proxy"(13) servers (where neither the spammer nor the recipients are local users). With the former method, ISPs will likely close down the accounts if they realize that they are being used for spamming activities, but usually not before hundreds of thousands or even millions of messages have been sent by the spammer. By using open proxies or open relays with a false e-mail address in the return message header to send e-mail anonymously, spammers can mask the true origin of the messages. In areas of the world where mobile phone text messaging (short message service, or SMS) is popular, such as Europe and Asia, spammers also send SMS spam to mobile phones.

---

(11) Paul Roberts "Sobig: Spam, Virus, or Both? Virus writer likely used spamming techniques to spread the worm quickly," *PCWorld*, June 2003, http://www.pcworld.com/news/article/0,aid,111028,00.asp.

(12) Open relays (also known as insecure relays or third-party relays) are configured to accept and deliver e-mail on behalf of any user anywhere, including third parties with no relation to the organization housing the server.

(13) Open proxy servers are misconfigured computers that allow traffic for virtually any network service to be channelled through a host computer. Spammers often identify and hijack such insecure proxy servers and use the computers to send huge volumes of messages anonymously.

Spammers obtain e-mail addresses by one of three methods: 1) by "scavenging," the practice of collecting (using automatic programs called "bots") e-mail addresses that are posted on Web pages and electronic bulletin boards; 2) by "guessing," in which the spammer uses dictionary terms or randomly generated strings to develop e-mail addresses; and 3) by purchasing e-mail addresses from list brokers.

CONTROLLING SPAM

A. Technological Options

There are various technological approaches that can reduce, but not eliminate, the delivery of spam to an ISP, a business network or an individual's home computer. At the most basic level, individuals and companies can write their own programs or rules to detect and eliminate spam. Many companies and ISPs invest in more sophisticated spam-filtering software (which may be Web-based, server-based or installed locally) sold by one of the many anti-spam software vendors that have sprung up over the last few years. There are various types of spam filters, including content analysis software that searches for such things as keywords, and behavioural analysis tools that look for spam patterns such as large numbers of recipients or blind copies. The newest spam filters are sophisticated programs that check messages against pre-established spam criteria held in a rules base, or statistical algorithms that "learn" the characteristics of legitimate e-mail vs. spam.

At another level, ISPs can subscribe to "blackhole" lists maintained by several companies.(14) These lists contain the Internet Protocol (IP) addresses of networks that originate or relay spam. Spammers are added to the lists following complaints and an investigation, and ISPs can then set their mail servers to reject messages coming from these IP addresses. A drawback of blackhole lists is that they are not selective, and all mail from spam-friendly networks is rejected, resulting in the loss of some legitimate messages.

Reducing the number of global open relays and open proxies could also help to curb the flow of spam. The U.S. Federal Trade Commission and other agencies in 26 countries recently announced "Operation Secure Your Server." As part of this international initiative, the participating agencies have identified tens of thousands of owners or operators of potentially

(14) See, for example, the Spamhaus Block List: http://www.spamhaus.org/sbl/index.lasso.

open relay or open proxy servers around the world, and are sending letters urging the owners and operators to close such servers and protect themselves from becoming unsuspecting sources of spam.(15)

Recently, the Chairman of Microsoft Corp. suggested that spam could be eradicated, via a technological fix, within two years. He announced that his company is examining ways to eliminate spam that include forcing senders of e-mail to pay a fee unless the recipient waives it.(16) Many analysts are sceptical about such eradication claims, arguing that no anti-spam technology is 100% effective, and pointing out that spammers are continually building new software applications to thwart anti-spam systems. For example, one of the latest spamming methods involves including random text written in white on a white background. This text is invisible to most recipients, but confuses filters that look for typical spam text.

B. Industry Self-regulation

Most Internet and direct marketing associations have, until recently, suggested that industry self-regulation should be sufficient to control spam. In Canada, the Canadian Association of Internet Providers (CAIP) supports such "self-regulatory initiatives." It suggests that government regulation or legislation cannot be flexible enough to keep up with the fast pace of technological change occurring on the Internet, nor is it able to operate across jurisdictions to respond to the borderless nature of the Internet. The Association has issued a document that lays out a series of "fair practices" for its members. One of the policies states that "CAIP Members will not knowingly allow their services to be used for the transmission of unsolicited bulk e-mail, especially unsolicited commercial bulk e-mail between parties that have had no previous commercial relationship."(17) Most major ISPs do have policies that prohibit spamming activities, and ISPs can terminate the account of any subscriber that is found to be engaging in such activities.

---

(15) U.S. Federal Trade Commission, "FTC and International Agencies Announce 'Operation Secure Your Server,'" 29 January 2004, http://www.ftc.gov/opa/2004/01/opsecure.htm.

(16) CBSNEWS.com, "Gates: Spam To Be Canned By 2006," 24 January 2004, http://www.cbsnews.com/stories/2004/01/24/tech/main595595.shtml.

(17) Canadian Association of Internet Providers, Self-regulation, http://www.caip.ca/issues/selfreg/subset.htm.

The *Code of Ethics and Standards of Practice* of the Canadian Marketing Association (CMA) prohibits its 800 members from transmitting marketing e-mail without the consent of the recipient or unless the marketer has an existing relationship with the recipient (a so called "opt-in" approach to marketing). Members can send marketing e-mail to existing customers, but such e-mail must clearly identify the marketer and provide the recipient with a simple means to reply to the marketer via e-mail. Additionally, members are prohibited from sending e-mail to recipients who have indicated they do not wish to receive further communications.(18)

In January 2004, Canadian federal, provincial and territorial ministers responsible for consumer affairs endorsed a voluntary *Canadian Code of Practice for Consumer Protection in Electronic Commerce*(19) that was developed by a working group of Canadian businesses, government and consumer organizations. The Code includes the following "principles" on sending unsolicited, commercial e-mail: 1) "Vendors shall not transmit marketing e-mail to consumers without their consent, except when vendors have an existing relationship with them. An existing relationship is not established by consumers simply visiting, browsing or searching vendors' Web sites"; and 2) "Any marketing e-mail messages vendors send shall prominently display a return e-mail address and shall provide in plain language a simple procedure by which consumers can notify vendors that they do not wish to receive such messages."

In the United States, members of the Direct Marketing Association (DMA) are not prohibited from sending unsolicited e-mails, but they must first purge their e-mail lists of the addresses of individuals who have registered with the DMA's "e-mail Preference Service" database. Marketers who are not members of the DMA can also have access to the database. Canadians who wish to have their e-mail addresses removed from such lists can sign up for this service.(20) Marketers belonging to the DMA must also provide individuals with a link or notice in each e-mail allowing the recipients to request that the marketer not send them e-mail in the future. In this "opt-out" system, the onus is on the recipients of spam to request that their addresses be removed from marketers' lists. The message should also disclose the marketer's

---

(18) Canadian Marketing Association, *Code of Ethics and Standards of Practice*, http://www.the-cma.org/consumer/ethics.cfm#Media.

(19) Working Group on Electronic Commerce, *Canadian Code of Practice for Consumer Protection in Electronic Commerce*, January 2004, http://cmcweb.ca/epic/internet/incmc-cmc.nsf/vwapj/EcommPrinciples2003_e.pdf/$FILE/EcommPrinciples2003_e.pdf.

(20) See instructions at: http://www.dmaconsumers.org/consumers/optoutform_emps.shtml. There is no cost for individuals who wish to sign up for the service. Marketers must pay a fee to the DMA to access the database.

identity, and the subject line should be "clear, honest, and not misleading."[21] Under federal legislation that took effect in the United States in January 2004 (see section below, "United States"), all commercial spam must now contain opt-out instructions and honest subject lines.

Self-regulatory schemes have done nothing to slow the flow of spam on the Internet. Spammers who are based abroad, who do not belong to national marketing organizations, or who are sending deceptive or fraudulent messages generally have no interest in adhering to code of conduct guidelines. For this reason, many jurisdictions have turned to legislation as a supplementary anti-spam weapon.

C. Legal Approaches

1. Spam Control Legislation

Different jurisdictions around the world have used one or more of the following general legislative approaches in an attempt to regulate spam: 1) banning e-mail with fraudulent or misleading headers or subject lines; 2) requiring spammers to include "opt-out" instructions with unsolicited, commercial e-mail messages so that recipients can request that spammers not send further messages; 3) requiring e-mail subject lines to carry labels if the message is an unsolicited advertisement; and 4) prohibiting the sending of unsolicited, commercial e-mail unless the sender has the prior consent of the recipient ("opt-in" approach). Spam control legislation has been introduced in several countries, including the United States, Australia and member states of the European Union. The legislative approaches taken in the United States and Europe, and the situation in Canada, are discussed below.

a. United States

Prior to 2003, there were no federal spam-related laws in the United States, although several anti-spam bills had been introduced in Congress over the previous few years[22] and 36 states had some form of spam control legislation on their books.[23] The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (or the CAN-SPAM Act of

(21) *DMA Guidelines for Ethical Business Practice*, April 2002, http://www.the-dma.org/library/guidelines/ethicalguidelines#6a.

(22) See summary at: http://www.spamlaws.com/federal/index.html.

(23) See summary of U.S. state laws at: http://www.spamlaws.com/state/index.html.

2003)[24] was enacted on 16 December 2003 and took effect on 1 January 2004. This legislation requires unsolicited, commercial e-mail messages to be labelled (although not by a standard method) and to include opt-out instructions and the sender's physical postal address. It prohibits the use of deceptive subject lines and false headers in such messages. It also prohibits the relaying of commercial e-mail messages via a protected computer or computer network that the sender has accessed without authorization. Under the law, the Federal Trade Commission is required to plan, and authorized (but not mandated) to establish, a "Do-Not-E-mail registry." The law also requires the Federal Communications Commission to introduce rules that protect consumers from unwanted, commercial SMS. The legislation supersedes state laws that require labels on unsolicited, commercial e-mail or prohibit such messages entirely, although provisions merely addressing falsity and deception would remain in place. Fines and/or prison terms may be imposed for violations of the law.

Some critics of the U.S. federal legislation have dubbed it the "YOU-CAN-SPAM Act," arguing that it legalizes spamming as long as spammers provide recipients with a way of "opting out." Critics note that the legislation supersedes state laws that were often stricter than the federal law. For example, California and Delaware both had laws that prohibited sending unsolicited, commercial e-mail from within those states or to recipients living in those states.[25]

Recent analyses of spam traffic suggest that the new legislation has not had any immediate impact on spam levels in the United States. According to three spam-filtering vendors, between only 1% and 10% of spam sent to U.S. addresses in the week following the introduction of the law in January 2004 complied with the legislation's labelling requirements. Furthermore, one vendor indicated that the volume of spam sent over that period actually increased.[26] Analysts suggest that strict enforcement of the law is essential if it is to have any effect.

---

(24) Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the CAN-SPAM Act of 2003), Public Law 108-187, http://www.spamlaws.com/federal/108s877enrolled.pdf.

(25) See, for example, the Spamhaus Project, "United States set to Legalize Spamming on 1 January 2004," http://www.spamhaus.org/news.lasso?article=150.

(26) Grant Gross, "Is the CAN-SPAM Law Working? Only a small percentage of unsolicited e-mail complies with the new law, studies show," *PCWorld*, 13 January 2004, http://www.pcworld.com/news/article/0,aid,114287,00.asp.

b. European Union

In July 2002, the European Parliament and the Council of the European Union adopted a directive(27) that is intended to provide a common level of protection across the member states of the European Union (EU) against unsolicited, electronic communications (FAX, automated calling machines and e-mail, including SMS) sent for the purposes of direct marketing. The directive is an "opt-in" approach whereby marketers are prohibited from sending e-mail without the prior consent of the recipient, unless the marketer has an existing relationship with the recipient. Marketing e-mail must clearly identify the sender and provide a valid address to which the recipient may send a request that such communications cease. The EU directive applies to "natural persons" (i.e., individuals); member states are also required to ensure that the legitimate interests of other subscribers (e.g., companies) are sufficiently protected by national legislation. The directive was intended to have been implemented by EU member states by October 2003. In November 2003, however, the European Commission launched infringement proceedings against nine member states because they had failed to make the EU directive part of their national legal codes.(28)

c. Canada

There are currently no federal laws in Canada that specifically target spamming activities, although news reports suggest that the government is considering whether to introduce such legislation.(29) Most spam sent in Canada, although annoying, is not illegal. However, sending spam that is fraudulent, or that involves unauthorized access to and use of computers, or mischief with respect to computer data, can be targeted under the *Criminal Code*. Additionally, the *Competition Act* contains provisions that prohibit misleading representations and deceptive marketing practices, including those made on the Internet. Finally, the *Personal Information*

---

(27) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

(28) European Commission, "Commission launches infringement proceedings against nine Member States for not adopting new privacy rules for digital networks and services," 5 December 2003, http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/03/1663|0|RAPID&lg=EN&display.

(29) Canadian Press, "Industry minister willing to consider law against unsolicited e-mails," 4 February 2004.

Protection and Electronic Documents Act establishes rules that govern the collection, use and disclosure of personal information during commercial activities. E-mail addresses are considered to be personal information and are therefore subject to the provisions of the Act.

Two spam-related bills were introduced by private members during the 37th Parliament. Bill S-2, An Act to prevent unsolicited messages on the Internet,(30) was introduced in the Senate on 3 February 2004.(31) If enacted, this law would allow the Minister of Industry to establish a self-governing council, to which all ISPs must belong, that would set ethical standards for its members and standards for spam(32) filtering. The bill requires the Minister to establish and maintain a confidential "no spam" list. Sending unsolicited e-mail to an address on this list, or sending e-mail that has a fake address or contains false information about any goods and services advertised, would be liable to punishment by a fine. For fraudulent spam, spam that is directed at children, or spam that contains child pornography or explicit sexual content, the proposed legislation allows for stiffer penalties, including imprisonment.

Bill C-460, An Act to amend the Criminal Code (unsolicited electronic mail),(33) was introduced in the House of Commons on 2 February 2004.(34) This bill seeks to amend the *Criminal Code* to create two new offences: sending unsolicited, commercial electronic mail (unless a prior business relationship exists) and selling electronic mail addresses without the prior consent of the persons affected. It provides for a sentence of imprisonment and/or a fine for a person convicted of either one of these offences.

Many consumer associations (e.g., the Canadian Coalition Against Unsolicited Commercial Email in Canada) have been calling for federal legislation to help curb the spam problem. Even some direct marketing groups are now suggesting that self-regulation may not be sufficient to control spam. The CMA suggests that legislation is an "option," provided it is harmonized with laws in other countries and across the provinces. It also notes that international

---

(30) Bill S-2, An Act to prevent unsolicited messages on the Internet, http://www.parl.gc.ca/37/3/parlbus/chambus/senate/bills/public/S-2/S-2_1/S-2_cover-e.htm.

(31) Originally introduced as Bill S-23 in September 2003 during the 2nd session, 37th Parliament.

(32) The bill defines spam as "one or more unsolicited messages sent and received on the Internet, but does not include a message sent by a person to another person with whom they have an existing commercial or personal relationship."

(33) Bill C-460, An Act to amend the Criminal Code (unsolicited electronic mail), http://www.parl.gc.ca/37/2/parlbus/chambus/house/bills/private/C-460/C-460_1/C-460_cover-e.html.

(34) Originally introduced under the same number in October 2003 during the 2nd session, 37th Parliament.

cooperation is necessary as spammers often operate outside Canada, raising jurisdictional questions.(35) In the United States, the DMA, which initially opposed the introduction of any anti-spam legislation, supported the federal CAN-SPAM Act. Critics of the DMA's about-face suggest that it lent its support to the legislation only because the law mirrors the DMA's existing rules on spam, which do not prevent its members from sending unsolicited, commercial e-mail.

d. Legislation and International Co-operation

Although legislation has been introduced in a number of countries around the world, it is not uniform, and differences among national laws compromise their effectiveness. For example, the U.S. legislation permits unsolicited, commercial e-mail to be sent to anyone unless the recipient explicitly requests that the messages stop. On the other hand, the EU directive requires prior consent from the recipient before any direct marketing messages can be sent. Analysts suggest that since the majority of the world's spam originates in the United States,(36) and because the U.S. law is weaker than the EU directive, EU residents will continue to receive large volumes of spam from addresses in the United States.

Given the borderless nature of the Internet, legislation may lead to a reduction in the amount of spam, but not its elimination. Spammers operating abroad may not abide by the legislation of other countries, and spammers who send their messages via foreign open proxies and who violate domestic laws may be difficult to trace or identify in order to lay charges.

There are some international efforts to curb the flow of spam, at least the deceptive variety. For example, in 2002, the United States Federal Trade Commission, eight state law enforcement agencies and four Canadian agencies joined together in an initiative called Netforce to target deceptive spam and Internet fraud. The agencies have focused their enforcement efforts on various Web-based scams ranging from auction fraud to bogus cancer cure sites, and have sent letters warning people that sending deceptive spam is illegal.(37)

---

(35) CMA response to Industry Canada's discussion paper *E-Mail Marketing: Consumer Choices and Business Opportunities*, http://www.the-cma.org/media/downloads/March%2027%20submission.pdf.

(36) In March 2003, 58.4% of spam received in the world originated in the United States, followed by China (5.6%), United Kingdom (5.2%), Brazil (4.9%) and Canada (4.1%). United Nations Conference on Trade and Development, *E-Commerce and Development Report 2003*, p. 27, http://www.unctad.org/en/docs//ecdr2003_en.pdf.

(37) U.S. Federal Trade Commission, "International Netforce Launches Law Enforcement Effort," 2 April 2002, http://www.ftc.gov/opa/2002/04/spam.htm.

2. Litigation

In many jurisdictions, lawsuits have been brought against spammers, largely by ISPs that have had their servers clogged with spam, or by third parties whose names or resources have been used without permission.(38) Most of these lawsuits have been in the United States, and a number of them have been successful.(39) The new federal anti-spam legislation enacted in the United States confers a civil right of action on the Federal Trade Commission, state attorneys general and ISPs, but not on individuals.

In Canada, a few spam-related lawsuits have made the headlines. In 1999, for example, an Ontario-based ISP took a subscriber to court for sending spam, which was against the ISP's policies. The spammer is said to have sent about 600,000 e-mails over a period of a few weeks that peddled a moneymaking scheme. The court ruled in favour of the ISP.(40) In another case, also in 1999, an Ontario ISP was sued by a client because the ISP had terminated its service. The ISP had done so because the client had allegedly been sending up to 200,000 unsolicited, commercial e-mails each day. The judge denied the client's motion requesting the ISP to restore service, saying that sending unsolicited, bulk, commercial e-mail is in breach of "Netiquette" principles, unless such a practice is specifically permitted in the governing contract.(41)

THE CANADIAN FEDERAL GOVERNMENT'S POSITION ON SPAM

Industry Canada produced a policy document on spam in 1997.(42) At that time, spam was not a serious problem and the document was intended to be largely for information purposes. The federal government believed then that a combination of current policy and legal frameworks, technological solutions, consumer awareness, and responsible practices by Internet industry stakeholders were sufficient to deal with computer abuse and criminal activity, including that involving spam.

---

(38) David Sorkin, "Technical and Legal Approaches to Unsolicited Electronic Mail," *University of San Francisco Law Review*, vol. 35, Winter 2001, pp. 325-384.

(39) See description of selected of cases at: http://www.spamlaws.com/cases/ and http://legal.web.aol.com/decisions/dljunk/otherarchive.html.

(40) Joaquim Menezes, "Ontario court sends spammer a message," *Computing Canada*, April 1999.

(41) Dan Goodin, "It's OK to cancel spam accounts," CNETnews.com, July 1999, http://news.com.com/2100-1023-228210.html?legacy=cnet.

(42) Industry Canada, *SPAM Discussion Paper – July 1997 Internet and Bulk Unsolicited Electronic Mail*, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/SPAM_1997En.pdf/$FILE/SPAM_1997En.pdf.

By mid-2002, however, it was estimated that the volume of spam had grown to at least 30% of total e-mail traffic, and was continuing to increase rapidly. Industry Canada then began discussions with some industry stakeholders, including marketers and ISPs, about possible methods of controlling the spam problem. In January 2003, Industry Canada issued a discussion paper on spam(43) that was sent to a small number of organizations representing ISPs, information technology industries, businesses and consumers. The paper raised a number of questions relating to government policies, enforcement of existing laws, network technologies, industry business practices, and consumer education and awareness. Further government consultations on the issue are expected in 2004.

CONCLUSION

Unsolicited and unwanted e-mail, more commonly known as spam, has become a major problem in recent years for both individual and corporate users of the Internet. Issues include the questionable content of a large proportion of spam, the financial cost of dealing with it, the displacement of legitimate e-mail by spam, and the threat it poses to the reliability and security of the Internet. Market-based approaches to regulating spam have done little to stem its flow, and individuals and companies have to pay, either indirectly (e.g., through lost productivity) or directly (e.g., for anti-spam technologies), to deal with it. A variety of anti-spam technologies have been developed, but none is 100% effective, and spammers are continually building new software applications to thwart anti-spam systems.

In recent years, governments around the world have begun to introduce legislation in an attempt to manage spam. The Canadian federal government has not introduced any legislation that specifically targets spam, but two spam control bills were introduced in Parliament by private members in 2004. The federal government's most recent policy statement on spam suggests that existing legislation, technologies and industry practices are sufficient to control it. Industry Canada has, however, been consulting with stakeholders about the spam problem and is currently reviewing its policy on the issue. Although legislation may help reduce the volume of spam emanating from some jurisdictions, it is likely that spammers (especially

(43) *SPAM Discussion Paper – January 2003 E-mail marketing: Consumer choices and business opportunities*, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/SPAM_2003en.pdf/$FILE/SPAM_2003en.pdf.

those sending deceptive, fraudulent or offensive messages) will continue to try to beat the system by sending spam from or through jurisdictions that have weak or no spam legislation, or where finding and prosecuting spammers is not a priority.

It is doubtful whether a single line of attack will substantially reduce global spam traffic. A multi-faceted approach that includes anti-spam technologies, industry cooperation, harmonized global legislation, stiff penalties for illegal spamming, cooperation across borders and consumer education is probably the only way that the global spam problem will be brought under control.