

SPAM Discussion Paper - January, 2003

E-mail marketing: Consumer choices and business opportunities

Introduction:

While technological progress has opened numerous new opportunities in on-line services, one of the oldest and most basic Internet applications, electronic mail, remains the most widely used. It is estimated that some 31 billion messages were sent over the Internet, in 2002, and that the number will reach or surpass 60 billion in 2006. For millions of people around the world, including those with limited access to the Internet, electronic mail has become the way to communicate and exchange information.

Electronic mail has also transformed the way companies and other organizations conduct their business. It provides a quick and efficient tool for internal communications and information sharing, even in companies and organizations whose operations span the globe. While new technological developments have made new communications tools readily available, such as videoconferencing, electronic mail remains the dominant medium in enterprise communications.

Electronic mail has also dramatically **changed the relationship between consumers and the suppliers** of products and services. In many industries, it has become one of the most cost efficient way of providing customer support and assistance. It also allows companies to quickly inform their customers of new products and services. Some are even predicting that permission-based Internet marketing, through electronic mail, could become one of the most important commercial Internet applications.

However, as is often the case when a new technology appears, abuse is not far behind. The use of the Internet to send large volumes of e-mail to promote products and services, while not illegal, has infuriated many consumers, forced employees in organizations to waste precious time deleting junk e-mail, strained the facilities of service providers and hurt the business of legitimate Internet marketers. A study done by the [European Commission](#) estimates that the cost of abusive e-mailing exceeds 10 billion Euros (\$14 billion Cdn. It is estimated that junk e-mail, that accounted for about 10% of Internet traffic, just two years ago, now amounts for 30 % or more. Most abusive e-mail promotes get-rich-quick schemes, for example how to get rich by sending bulk commercial e-mail. Some are clearly fraudulent, for example promoting pyramid and bogus no-risk investment schemes; others, like those advertising "miracle" diet and health products, are misleading and deceptive.

Many studies have shown that electronic mail marketing when, done appropriately, can be highly effective. This is particularly the case where marketers have obtained the permission of consumers, are able to target their messages to those who have expressed an interest in a particular product or service, and, at the very least, provide recipients with the opportunity of having their names removed from future mailings. Members of the [Canadian Marketing Association](#) (CMA), who abide by an industry Code, will only solicit consumers with whom they have an existing relationship. The CMA also manages an e-mail preference program that allows consumers to have their name and address removed from marketing lists. However, because the sender only incurs minimal costs for sending hundred of thousands, or even millions of e-mails, in

a totally indiscriminate fashion, abusive electronic mailing may remain an issue for some time. Furthermore, many abusive e-mailers appear to provide recipients with an option of having their name removed while, in fact, using the reply as a means of validating an e-mail address. Thus, the consumer who replies is likely to get more commercial solicitation.

In 1999, Industry Canada put online an information document on [bulk unsolicited commercial electronic mail](#) which stated that the application of existing laws, appropriate Internet industry policies, technology and consumer awareness could, to a large extent, deal with abusive electronic mailing. With the significant rise in the volume of junk e-mail experienced in the last two years, the department began, in 2002, discussions with some industry and consumer stakeholders as part of a review of its current policy.

In these preliminary discussions with stakeholders, one of the issues that emerged was the difficulty of **defining what is spam**. Not all participants agreed with the general definition of "unsolicited commercial e-mail". Some expressed the view that a definition should be based on the volume and indiscriminate nature of commercial e-mail and not only on whether this communication was solicited or not. However, all agreed that finding a commonly accepted definition was an essential element of any proposed solution.

In 2002, the [Australian National Office for the Information Economy](#) (NOIE) encountered the same difficulty when it conducted an extensive review of the spam issue. In its review, NOIE, while recommending further work on a widely recognized and accepted definition, did develop a **working definition: it defined spam e-mail as a communication that could not be reasonably assumed to be wanted or expected by a recipient.**

Through these consultations, the department has identified a number of other issues that would warrant discussion by the broad range of stakeholders.

Real Consumer Choices

Under the [Personal Information Protection and Electronic Documents Act](#), which came into force on January 1, 2001, electronic mail addresses are considered personal information and thus are subject to the provisions of the Act. In October 2002, the [Privacy Commissioner](#) found a number of major organizations that provide communications services at fault for failing to obtain meaningful consent from their customers before using their addresses for secondary purposes, such commercial solicitation.

While the great majority of Internet and electronic mail service providers make some reference to the use of their subscribers addresses for commercial purposes in their Terms of Agreement, these provisions are often unclear and not displayed prominently. Many subscribers would be surprised to discover that they have agreed, by default, to receive some form of commercial solicitation.

Discussion points:

Since they are the first point of contact between consumers and Internet services, like electronic mail, do Internet service providers (ISPs) and other e-mail service providers have a responsibility or a role in the management of their customers e-mail preferences?

By using existing technology, could ISPs and other e-mail service providers require that a potential customer register his or her electronic mail preferences before activating an account?

On the basis of these expressed preferences, could ISPs and e-mail service providers, individually or collectively, play a active role in the distribution of commercial solicitation to their customers?

Is there a role for ISPs and e-mail service providers in establishing or managing benefit programs for customers who agree to receive commercial solicitation?

Filtering Technologies

The **rapid growth in the volume of junk e-mail** has led to an increased demand for filtering technologies. While such technologies have existed for years, many for individual users, most of the new services offered on the market are aimed at service providers and organizations. Some claim an 80% plus success rate in intercepting junk e-mail. However, while certain key words and features make it relatively simple to intercept e-mail that promote adult entertainment or some get-rich-quick schemes, abusive e-mailers have shown themselves to be resourceful in getting through security firewalls and filters. The most effective e-mail filtering services, however, can entail considerable added costs for service providers and, in the end, for consumers.

Discussion points:

Should e-mail filtering, to consumers or at a network level, be considered as part of basic electronic mail service or be offered, at a cost, as a premium service?

Is there any merit in bundling effective e-mail filtering with other security enhancements as a premium service?

Can current technology allow the identification of legitimate e-mail solicitation?

Is there any merit in ISPs and legitimate marketing industries cooperating in developing and implementing the use of such technological tools to increase the effectiveness of filtering services?

Appropriate Policies

The vast majority of ISPs and e-mail service providers have adopted strict anti-spam policies. In their Terms of agreement, they maintain the right to terminate the account of any subscriber who engages in abusive e-mail practices. However, those who choose to engage in bulk unsolicited commercial e-mail, appear to have very little difficulty in obtaining new accounts, if they are cut-off by a provider as a result of e-mail abuse.

Discussion points:

Are there further steps that could be taken to ensure that a zero-tolerance policy is effectively enforced industry wide, through domestic and international cooperation?

If so, what role could industry or governments play in developing these measures?

Should Internet users be clearly advised of the possible consequences of e-mail abuse, such as denial of service by other providers?

Network Solutions

The benefits of the Internet as a global network of networks are well known. Those who choose to abuse this technology, for example for indiscriminately sending bulk commercial e-mail, have also taken advantage of the configuration of Internet networks. In the early days of the Internet, the computers that directed traffic were configured to relay communications without discrimination. As

networks have evolved and multiplied, this function is no longer required and many providers have configured their facilities accordingly. However, abusive e-mailers have found ways of identifying and using facilities that are not configured appropriately and to use them as relays for distributing their communications. Thus an abusive e-mailer in North America could use an improperly configured server in, for example, Asia, to relay one million or more e-mails to American customers. Some service providers have taken steps to curtail this abuse, for example, by refusing to accept communications traffic from improperly configured servers or even from countries where a large number of facilities can be used for relaying inappropriate communications.

What role could the Internet service industry and information technology suppliers play, through various international Internet governance or technical fora, in developing and implementing best practices for configuring network facilities, to curtail abuse such as indiscriminate bulk commercial e-mail?

A Role for Government

In its 1999 position document, the government indicated that the use of electronic mail for commercial solicitation was not illegal, any more than commercial solicitation through traditional mail. Furthermore, it noted that advertising, while subject to laws of general application, such as the *Criminal Code* and the *Competition Act*, is only regulated in areas under federal authority, like broadcasting.

In the case of **telemarketing**, by telephone or facsimile, federal broadcasting and telecommunications regulator, the [Canadian Radio-Television and Telecommunications Commission](#) (CRTC), instructs facilities based carriers under its jurisdiction to terminate the service of those who do not abide by the Commission's rules. Retail services provided by ISPs are not subject to CRTC regulation.

In the last two years, a number of jurisdictions have taken legislative or regulatory action to curtail junk e-mail. While none of these measures specifically prohibit solicitation by e-mail, they are aimed at, for example, in the European Community, forcing e-mail marketers to obtain consumer consent. In the United States, some 26 state governments have enacted laws that go from prohibiting falsified return addresses, requiring clear advertising labels and giving recipients and governments the right to sue for specified damages. In Canada, there have been calls for legislative or regulatory action.

Should new laws be enacted in Canada?

If so, what activities should be targeted?

- Should the use of e-mail for commercial solicitation be prohibited, in some or all instances?
- Should the use of e-mail to acquire new customers be prohibited?
- Should the option of refusing further solicitation be required?
- Should the use of falsified return e-mail addresses be prohibited?
- Should e-mail commercial solicitation be required to be clearly labelled as advertising?

- Should providers or individuals be allowed to seek specified damages for junk e-mail?
- Should software products used for collecting e-mail addresses, transmitting bulk e-mail and falsifying return addresses be controlled or banned?

Applying existing laws

While there have been no reported occurrences, large volumes of junk e-mail could interfere with critical computer systems and endanger public safety. Such an occurrence could lead to mischief charges under the *Criminal Code*. A conviction for such a serious offence is punishable by up to ten years in jail.

The collection and use without consent of personal information, such as e-mail addresses, could run counter to the requirements of the *Personal Information Protection and Electronic Documents Act*. The [Privacy Commissioner of Canada](#) is entrusted with enforcing the *Act*. However, the privacy legislation applies only to organizations located in Canada and the rules concerning the collection and use of personal information varies widely from country to country. The [European Union](#) has deemed the provisions Canadian privacy legislation to be adequate to allow the exchange of personal information.

It remains, however, that software designed for collecting e-mail addresses and compact disks containing thousands or hundred of thousands of addresses are widely available on the Internet and by direct mail. Some of the junk e-mail in fact promotes these products as a way of earning extra income. While much of the junk e-mail might be considered misleading or deceptive, some communications, like those promoting pyramid investment schemes, are clearly fraudulent under existing laws. Others, for example those promoting adult entertainment products and services, are, while not illegal, not appropriate for young children. Since many abusive e-mailers make no effort to target recipients, young children are more than likely to be exposed to these messages.

In the United States, the [Federal Trade Commission](#) has launched a active enforcement campaign against senders fraudulent e-mail (scam). The FTC has initiated a number of prosecutions and shut down a number of schemes through consent orders. There is no such national organization in Canada. The [Royal Canadian Mounted Police](#) and local law enforcement agencies, working through the [Phonebusters National Call Centre](#) have taken action in a number of cases, mostly by intervening with Internet service and mail providers. Because many of these fraudulent proposals emanate from other countries, the investigation and prosecution of these cases is very difficult.

Should establishing a central Internet-based reporting system for fraudulent and other illegal e-mail be considered?

If such a central system was established, who could most usefully fund and manage it

Consumer Awareness

No matter how many laws are enacted and regulations imposed, the Internet, by its architecture and reach will always present enforcement challenges. For this reason, as indicated in the 1999 government information document, well informed consumers will remain a key element in the orderly development of the Internet and its use.

Many products and services on the Internet are provided with no charge to the users. However, consumers should bear some responsibility for taking the time to verify what conditions may be attached to these free products and services. Most organizations who maintain web sites on the Internet have now developed privacy policies that will explain how personal information provided by their customers will be protected or used for other purposes. Whether such privacy policies are clearly visible and written in plain language varies considerably from web site to web site. In fact, many purported free products and services do have a price and that price might be unsolicited commercial electronic mail.

Consumers should also be aware that certain areas of the Internet, like newsgroups, have no or very little security. Each day, millions of Internet users from around the world exchange views and ideas on a wide range of subjects. At the same time, they expose their e-mail addresses to public view. As a test, the United States Federal Trade Commission recently posted messages on newsgroups using assumed e-mail addresses. In some instances, less than eight minutes elapsed before junk e-mail began arriving at these addresses. In order to make informed choices, consumers require clear and precise information regarding the services, including commercial e-mails, that may form part of a bundle of apparently "free" services offered on the Internet.

The Principles for Consumer Protection for Electronic Commerce - A Canadian Framework were developed by the Working Group on Electronic Commerce and Consumers. The working group included governments, consumer and business associations and its work was coordinated by the Office of Consumer Affairs of Industry Canada. The [Principles](#) were approved by the working group in August 1999 in order to guide the development of a consumer protection framework for electronic commerce over open networks, including the Internet. **Principle 7** addresses Unsolicited Commercial E-mail and says, "Vendors should not transmit commercial E-mail without the consent of consumers, or unless a vendor has an existing relationship with a consumer." On this point, the *Principles* are consistent with the *Guidelines For Consumer Protection in the Context of Electronic Commerce* developed by the [Organisation for Economic Cooperation and Development](#) (OECD).

What further steps could be taken to better inform Internet users on how to curtail e-mail abuse?

Who should be responsible for public education on e-mail abuse?

What role could industry stakeholders and governments play in improving public education?

Conclusion

The preceding questions relate to some of the issues raised in preliminary discussions with stakeholders. In some cases, these consultations clearly indicated that some of the issues had not been fully discussed even within some industry groups. In other cases, it was also clear that there had been no meaningful dialogue between these industry groups on finding common solutions. However, all were in agreement that if these issues were not addressed at a broad level, many of the efficiencies gained through the use of e-mail would be greatly diminished as consumer suspicion grows with the flood of unsolicited commercial electronic mail.

The purpose of the preceding questions is to engage this dialogue to identify possible areas where both industry stakeholders and consumers will find a common interest in achieving effective solutions.

Please send comments to: spam_paper@ic.gc.ca

Note: While no formal deadline was set, the Department hopes that stakeholders will be able to provide their comments on the Discussion Paper by mid-March 2003.