An Anti-Spam Action Plan for Canada

The Problem

In just a few years, unsolicited commercial e-mail -- now generally known as "spam"[1] -- has gone from being a minor nuisance to becoming a significant social and economic issue, and a drain on the business and personal productivity of Canadians. Spam now impedes the efficient use of email for personal and business communications, and threatens the growth and acceptance of legitimate e-commerce.

Consider:

- In the year 2000, email traffic reports indicated that spam amounted to about 10 per cent of the total volume of electronic mail.

[1] The terms "spam" and "unsolicited commercial email" are used interchangeably in this document.

The Task Force will work with the Privacy Commissioner of Canada to assess whether Canadian organisations that collect and use e-mail addresses have developed appropriate practices and procedures, as required by PIPEDA, and to identify any corrective actions that may be needed to reduce and control spam.

(ii)The Criminal Code and the Competition Act

Sending unsolicited commercial e-mail for a legal product or service is currently not a criminal offense. Like unsolicited commercial information distributed through traditional mail, it can be considered a form of advertising and marketing. The current *Competition Act*, however, contains specific provisions dealing with deceptive and misleading representations that have frequently been used to deal with misleading advertising in traditional media. The application of the Act to misleading claims made in e-mail solicitations is an area that merits examination.

Similarly, many e-mail abusers now resort to forged information in electronic mail headers to avoid being identified, and the sending of “trojan” programs embedded in e-mail messages that can be activated by spammers to relay spam. Such methods of gaining unauthorized access to computer systems could violate several current provisions of the *Criminal Code.* These provisions provide for substantial fines and even imprisonment. Whether evidence of intent to commit criminal fraud through spam could be proven is unclear. This application of this law to spam, however, merits examination.

well, the Task Force will review existing laws to determine whether stronger enforcement or new legislation could make a significant impact on the reduction and control of spam, and whether the government should consider taking any further legislative or enforcement measures.

Network management practices, and industry codes

Any measure aimed at successfully curtailing the flow of unsolicited and unwanted commercial e-mail must involve more than government actions. There is now a growing consensus among stakeholders on a number of steps that can be taken by Internet service providers[2] and businesses who use the Internet to rebuild trust in e-mail communications.

Some of these initiatives relate to the development and application of technology, others to the implementation and enforcement of best practices within the

[2] For the purpose of this document, Internet service providers (ISPs) include private organisations that provide both connectivity as well as carriage of Internet communications, and other related services.

and adopt management practices that will effectively reduce and control spam.

Canadian industry stakeholders have the ability to agree on basic operating practices for network facilities that will reduce spam, and can show leadership by requiring their adoption on networks and facilities based in Canada. They should also encourage equipment makers and suppliers to configure their products in a way that does not facilitate abuse.

Industry Best Practices: Codes of Conduct

Over the years, Internet industry stakeholders have emphasized to consumers and to governments their ability to self regulate, and many have developed voluntary codes based on industry best practices. The government recognizes that these codes must evolve to reflect changing circumstances, particularly where technology and the very nature of services offered is changing quickly and constantly. However, many of these best practices initiatives, as they currently exist, remain at the level of suggestions for members of organisations.

The reality of Internet communications is that many firms are involved in any chain of commercial electronic solicitation, starting with the seller of goods and services, to marketers, bulk e-mailers, network carriage providers and finally, the operators of e-mail servers, such as ISPs and commercial organisations, that receive and store the communications.

In some cases, stakeholders in this chain have already developed agreements to ensure the movement of commercial e-mail. Some marketers and e-mailers negociate with ISPs to be “whitelisted” to ensure delivery of e-mamnentary *the viability of e-commerce, should provide clear information on acceptable commercial e-mail practices and policies, and should ensure that Internet users are provided with the tools they need to make informed choices.*

Systems to validate legitimate commercial communications

Up until now, most initiatives aimed at controlling the rising volume of unsolicited commercial e-mail have focussed on a combination of filtering technologies, and the use of so-called “blacklists” of servers and domains that have been identified as sources of spam. As these spam control services have become more and more sophisticated, so have the e-mail abusers who continue to find new tactics to bypass the barriers.

The diverse types of spam filtering and blocking tools, and the cyclical battles between spammers and spam blockers, have produced some unwanted results. In particular, legitimate commercial communications are now too often blocked inadvertently by filters, sometimes without the knowledge of either the sender or recipient. Legitimate noncommercial personal communications can also be blocked for the same reason.

These filtering practices, though well-intended, have therefore inadvertently contributed to undermining confidence in the reliability of e-mail. For this reason, a number of commercial organisations are now considering moving their services to closed networks.

There are, however, technical means of shifting the focus away from blocking unwanted communications toward facilitating the movement of legitimate commercial e-mail. Some of these verification systems are based on proprietary technology, but others are open source. While these programs may impose some costs on the senders of commercial e-mail, and on those who own and manage Internet network facilities, these costs would be more than offset, for senders, by the value of guaranteed delivery. Service providers would also see reduced costs in managing e-mail service and customer preferences. Validation protocols could also provide e-mail users with more effective tools to manage their own e-mail preferences, and reduce the risk of people receiving content they consider inappropriate.

While it would be inappropriate for government to limit the development of a competitive marketplace by endorsing one particular validation technology or protocol, the use of technology to validate legitimate commercial e-mail and to provide Internet users with effective choices is one of the most promising solutions to spam. For this reason, ISPs and businesses who use e-mail for *commercial activities have a shared interest in using technology to validate legitimate commercial communications. Requiring the true identification of the sender and the nature of the communication, as well as an effective means of refusing further e-mail from a verified sender, would be a minimum requirement for e-mail certification. Such a regime should also include effective performance measurement, and appropriate sanctions for certificate holders that do not abide by the rules.*

Consumer education and awareness

While there is much that industry and marketers can do that is effective in combatting spam, and seamless for e-mail users, there is general agreement among stakeholders that more should be done to inform Internet users on what they can do to limit the amount of unwanted commercial e-mail they receive.

While there is a considerable body of readily available information on best online practices to avoid spam, it appears, judging by the number of complaints recorded, that current efforts to communicate this information requires more effort. Some of the simplest messages – such as don't buy from spammers – have not reached some consumers. There is clearly a need for information to users that is credible, well-distributed and well-marketed.

Given the small positive returns needed to make spam commercially viable, consumer awareness of the relationship between spam and profits and their personal behaviour needs to be more strongly emphasized. While shifting most of the burdens of dealing with unsolicited junk e-mail to individual users, under the guise of user empowerment, is not a viable strategy to resolve the current crisis in e-mail trust and confidence, the government believes that there is need for more effort in this area.

Service providers and legitimate sellers of goods and services, because of their direct relationship with Internet users, are in the best position to lead a public education and awareness campaign, delivered in partnership with consumer groups and governments. To facilitate the development of an appropriate social marketing and communications program aimed at users, serious consideration should be given to supporting an effective private sector-led plan to achieve this objective, and to implementing it in conjunction with consumer groups, provincial governments, and interested international partners.

Supporting Global Anti-Spam Initiatives

For a number of years, the government has been active in several international fora where Internet issues have been discussed. Canada chairs a Joint Working Party within the Organisation for Economic Cooperation and Development (OECD) that is currently developing an action plan on unsolicited commercial e-mail. It has also been involved in relevant work of the Asia-Pacific Economic Cooperation (APEC) forum and by the business-led Global Business Dialogue on Electronic Commerce (GBDe).

Much of these international discussions have focussed on various legislative and regulatory actions taken by some countries to deal with the flood of unsolicited commercial e-mail, and the need to ensure that these approaches are compatible in the global Internet environment. While legislation is important, it is now clear that a broader approach – such as the more comprehensive approach discussed in this document – is needed at the international level.

Canada will continue to play a leadership role in international efforts to reduce and control spam. One of the major ways international efforts could prove more successful would be for member countries to more closely involve their domestic industries in these deliberations, and to broaden the global fight against spam to include a broader range of solutions. As this document makes clear, fighting spam here in Canada requires a partnership effort by government, industry and consumers. The same partnership collaboration is required internationally.

For this reason, the government supports the development and adoption of best practices for e-mail marketing and network management in an internationally coordinated manner. We also encourage the Canadian Internet and marketing industry, and Canadian consumer representatives, to become active in international efforts to reduce and control spam through initiatives such as the move toward globally compatible e-mail certification and validation regimes.

A Realistic Timetable

By its mandate, the Task Force has one year to oversee and coordinate the implementation of the Action Plan. After this period, the Task Force will report on progress made and propose any new actions that might be required, including legislative initiatives.

During the course of the next year, the Task Force will convene key stakeholders to review the implementation of the Action Plan and to identify any other possible areas that might require further action.

The Task Force will consult all interested stakeholders and individual Canadians who might wish to express their views or make a contribution to its work. It will report regularly on progress made and, if necessary, meet with organisations and groups representing key stakeholders.

Industry Canada
May 2004

Overview: Components of a Comprehensive Canadian Anti-Spam Initiative		
Need for international action to deal with spam as a global problem	Continued Government efforts at international level, involvement of Canadian partners with international counterparts	Government lead involving all partners.