



Global Business Dialogue on Electronic Commerce

Building Consumer Trust Unsolicited Electronic Communications (Spam) A Multilateral Framework

Issue Leader (Americas):

*Michael J. Sabia
President & CEO
BCE Inc.*

November, 2003

Introduction

The growth of the Internet has led to increased opportunities for education, communication, commerce and new employment opportunities; it has revolutionized the means of human interaction and has developed into an essential tool for the global realization of freedom of speech and the individual's right to receive and impart information¹⁵. However, the very qualities of the Internet which make it capable of advancing social and commercial objectives also make it susceptible to abuse.

Electronic mail or email, the oldest and most basic Internet application, remains the most widely used and, for millions of people around the world, has become the way to communicate and exchange information. Email has transformed the way organizations conduct their business, providing a quick and efficient tool for internal communications and information sharing. It has also changed dramatically the relationship between consumers and suppliers of products and services. Email is becoming, in

many industries, one of the most cost efficient ways of providing customer support and assistance, and allows companies to quickly inform their customers of new products and services.

Unsolicited email, or so-called "spam"¹⁶, is a growing worldwide problem with a direct impact on consumer trust in the Internet and significant economic cost for all stakeholders, thereby threatening the benefits and opportunities of a global Internet society.

The impact on consumers is felt at multiple levels: as receivers of unsolicited email who waste time and money sifting through unsolicited email and deal with the annoyance factor of receiving potentially offensive and sometimes illegal content; as users of the Internet who put up with slower access; as recipients whose email is mistakenly filtered out; as senders of email whose emails are blocked by other domains; as customers whose Internet access rates increase as a result of the costs

¹⁵ GBDe Tokyo Recommendations – Cyber Ethics – September 2001.

¹⁶ For the purposes of this document, "unsolicited electronic communications", "unsolicited email" and "spam" will be used interchangeably.

associated with unsolicited email; and as individuals who miss out on the benefits of an Information Society.

Internet service providers (ISPs) bear the infrastructure costs associated with both carrying and combating unsolicited email such as the need for increased bandwidth, additional and more sophisticated servers, filtering technologies including resources to manage these filters and the various unsolicited email lists, etc. ISPs are also concerned about the possible negative impacts on their brand. Many customers believe that their ISP is somehow responsible for the unsolicited email they are receiving or has the ability to stop it. Internal resources are therefore necessary to respond not only to customer complaints about incoming unsolicited email and slower traffic, but also to denial of service complaints when other service providers or domains have blacklisted an ISP's domain when one of its customers has engaged in sending unsolicited email. Ultimately, these costs put pressure on ISP price structures for customers.

As employers, not only do we bear infrastructure costs associated with firewalls and filters to keep unsolicited email from entering our internal networks, we are also faced with the cost of lost employee productivity and increased employee frustration. Our employees are also customers who have to deal with the problem of unsolicited email at home.

As commercial users of email, both to communicate with existing customers and to solicit new customers, we are concerned about the growing mistrust of legitimate commercial activity in this area and the possibility that efforts to address this increasing problem may have negative impacts on our ability to continue to use email for legitimate commercial purposes. Furthermore, there is the cost incurred by an increasing number of legitimate email marketers who see their emails being filtered.

The negative impact of unsolicited electronic messages is not simply an issue for traditional email, but is increasingly becoming a problem for other electronic services such as instant messaging, both online and to wireless devices,

and even extending itself to traditional voicemail systems.

Furthermore, the common problems of unsolicited email are manifesting themselves differently around the world. For example, in North America and Europe, spam has primarily been an issue of unwanted commercial messages and fraudulent schemes. Increasingly, however, unsolicited emails are also delivering harmful content. In Japan, unsolicited electronic communications are increasingly implicated with social concerns such as facilitating spontaneous teenage prostitution, group suicides or exploitation of the elderly.

Another relatively unique manifestation, resulting from the different allocations of computer code in Japan and China for the same Chinese characters, has introduced a new cross-border issue where Chinese-originated unsolicited email is completely unreadable by Japanese recipients, thereby increasing the annoyance nature of such emails as well as the increased impacts on available bandwidth.

The evolution of the Internet society has reinforced the need for a coordinated approach to problems as they arise. In order to substantially reduce the negative impacts of unsolicited electronic communications or spam, there is a need for a "tool kit" approach that combines self-regulation, technology, education, legal solutions and international cooperation involving government, business and civil society.

Defining Unsolicited Electronic Communications or "Spam"

At a very basic level "spam" could be defined as an electronic communication that is not likely to be wanted or expected by a recipient. However, any meaningful attempt to address the problem of unsolicited electronic communications necessarily requires everyone to come to some common understanding as to what it is we are really talking about and then to consider what aspects need to be addressed on a priority basis and by what means. Even though a great deal of energy has been devoted to the issue of defining spam over a number of years, there is no

universally accepted definition at the present time.

One of the dangers inherent in some current approaches to the problem is the grouping together of all marketing-based communications under the general heading of unsolicited email. A priority, therefore, must be for unsolicited electronic communications to be clearly defined to enable legitimate business communications to be separated from fraudulent, unsolicited communication. Separating the two will enable a much more consistent, coordinated and targeted policy response.

In this context, it is useful to consider some of the characteristics that are usually associated with unsolicited electronic communications and that can be grouped into four different categories:

a) recipient's expectations:

- unwanted or unexpected (i.e. without consent, either express or implied);
- no prior existing relationship with sender.

b) content of communication:

- annoying or offensive (e.g. chain letters, hoaxes, pornography, personal relationship advertising, spiritual);
- marketing or commercial;
- illegal or fraudulent (e.g. child pornography, get-rich-quick schemes, misleading advertising).

c) sender details:

- inability to know identity of sender or non functioning return path;
- no physical address or details provided for sender.

d) form of communication:

- inability to unsubscribe or opt-out of future communications;
- sent by bulk/mass distribution (e.g. use of automated means and sent in a largely untargeted and indiscriminate manner);
- method used to collect email address of recipient (e.g. harvesting the web for email addresses, attacks that monitor emails that do not bounce back);

- "brute force" or "dictionary" attacks that do not rely on collection of email addresses;
- inappropriate use of open relays.

However, having considered the characteristics of these four categories, a more productive approach may be to define unsolicited electronic communications in terms of behavior instead of the form or content of the message, or the receiver's expectations, thereby removing as much as possible any subjective elements to the classification of email as unsolicited email.

Building on Existing Consensus

It is commonly agreed that the most annoying unsolicited email involves deception of some kind, either in the content of the message, the identity of the sender, etc. By focusing on unacceptable and deceptive behavior, *unsolicited electronic communications* could be defined as electronic communication via any means that includes any or all of the following:

- absence of consent to receive either via opt-out or opt-in principles;
- harvesting of personal information;
- false information or claims including "subject" and "from" lines, as well as content;
- intent to defraud; or
- erroneous reply address information.

Including the bulk or mass nature as a characteristic of unsolicited email may no longer be effective as it imposes problems for legitimate commercial companies who use email to communicate with their customers and the most serious emailers are able to avoid this classification by breaking up the quantities of their mail sent into smaller groups.

Therefore, rather than debating points of difference, it is more productive to focus on those elements of unsolicited email upon which there is the most agreement.

Approximately 60% of all email includes false headers and deceptive content, emails that would easily fit within the above definition of unsolicited email. Taking this amount off the

table would allow positive movement in addressing the problem. In many countries, the enforcement of existing consumer protection legislation would go a long way to addressing the proliferation of such fraudulent electronic communications. Therefore, given the most serious and worst unsolicited emailers are also the most difficult to track, enforcement resources should tackle those who engage in deceptive behavior.

From a privacy perspective, this 60% of harmful email is really more a question of unwanted intrusion given the illegitimate and fraudulent nature of those emails. The less harmful 40% of emails is where data protection is likely to be more of an issue and where industry best practices will have the greatest impact¹⁷.

Need for a “Tool Kit” Approach

An information-based society requires increasingly sophisticated responses involving cooperation from all stakeholders. Although unsolicited email is unlikely to be eliminated from the lives of Internet users, whether fixed or wireless, it may yet be effectively controlled, managed and reduced through a combination of self-regulation, technology, education, legal solutions and international cooperation. It is generally agreed that a tool kit approach is necessary to address the increasing problem of unsolicited email and that all stakeholders have a role to play. Both the kind of tools and the roles of the various stakeholders will continue to change over time.

1. Self-regulation and Codes of Conduct

There are numerous voluntary practices that an ISP can consider to assist in addressing the problem of unsolicited email. Some practices are widely used today while others are being considered as the negative impacts of unsolicited email increase (see below). ISPs should be encouraged to consider such measures. However, given the varying sizes and resources of

¹⁷ GBDe Tokyo Recommendations - Consumer Confidence – Personal Data Privacy Protection, September 2001.

individual ISPs, the adoption of such voluntary measures should remain at the discretion of the ISP and should not be mandated by legislation. All stakeholders, including governments, law enforcement agencies and consumer groups, should seek to better understand the impacts of unsolicited email on the various players including ISPs, the measures available and the differing capabilities of the players to adopt such measures.

Given the recognized effectiveness of commercial email, legitimate commercial email users have a vested interest in adopting practices that clearly demonstrate that there is a difference between legitimate commercial email and unsolicited email.

2. Technology

The Internet industry has an interest in continuing to develop technological solutions to address this problem. Some technological solutions try to block unsolicited email before it reaches a user’s inbox while others try to filter it out after it has arrived. ISPs have an increasing interest to use filtering systems and make them available to their customers based on their own business models, e.g. as part of the service or as a separate service to customers.

However, one of the risks of any email filtering system lies in the possibility of falsely identifying "legitimate" mail as unsolicited email, known as "false positives". There are other downsides to these technological measures, e.g. many filters block the servers from which the unsolicited email originates but not the individual senders of unsolicited email.

Part of the solution to the long-term reduction of unsolicited email will include the availability of filtering technologies for end-users. New filtering products are being developed with increasing frequency and it is expected that widespread use, coupled with education strategies, will be an important element in empowering consumers to deal with the problem. Consumers, therefore, should be encouraged to

use technological solutions made available to them.

3. Awareness and Education

ISPs have a vested interest in educating their customers or users about protecting themselves against unsolicited email and explaining to them the measures they are taking to combat unsolicited email. Customers who are more aware and take steps to protect themselves are less frustrated and make fewer calls to complain to their ISP. On the flip side, customers or users who know that such activity will not be tolerated by their service provider may think twice before engaging in such activity or allowing others to make use of their computers to do so.

ISPs can use various methods to educate their users, e.g.: the development of detailed policies and practices, terms and conditions of service, and FAQs; making available specific information and relevant links; sending out reminders; and setting the right example by being clear in their own email communications with their own customers and users.

ISPs themselves should proactively seek out information about the problems and possible solutions to unsolicited email. Also, more proactive ISPs have a vested interest in raising the awareness among ISPs generally – for every unsolicited email message that an ISP can keep from leaving its network, it is one less message that enters another ISP’s network. At the industry level, there may be a role for associations to educate their members and users, and to cooperate with other similar associations around the world.

Consumer groups have a role in raising consumer awareness about the growing problem of unsolicited email and helping to find solutions to help fight unsolicited email. Consumers are also in the best position to determine whether email they receive is wanted or not. Parents should be encouraged to tell their children not to provide their personal information online including their email address. By increasing efforts to protect themselves, consumers can also contribute to decreasing the overall amount of

unsolicited email, e.g. by reporting unsolicited email. Consumers, therefore, have a clear incentive to educate themselves about the growing problem of unsolicited email.

Given the growing importance of electronic commerce to governments and to the well being of society generally, all levels of government have a key role to play in raising awareness about how consumers can protect themselves and contribute to decreasing the extent of unsolicited email. Awareness and education should also take place in the schools.

4. Legal Solutions

There are various types of legal solutions available to assist in combating the negative impacts of unsolicited email ranging from government enforcement and the pursuit of civil actions pursuant to existing laws, amendments to existing laws to ensure their effectiveness in addressing online problems and broader legislative initiatives.

The danger of relying purely on broader legislative initiatives is that new laws may have an unforeseen impact on electronic commerce and ultimately provide little deterrent effect on those who are engaged in deceptive behavior.

Furthermore, despite a general agreement for a multilateral strategy to address the increasing problem of unsolicited email, it appears there is still an apparent rush to new broader legislative initiatives on the part of some governments resulting in piecemeal legislation. In 1999, the GBDe cautioned governments that future regulations on unsolicited email should be internationally compatible¹⁸.

What is needed is a truly harmonized international approach to legislation that may, or may not, require Internet-specific legislation and that proves to be an effective tool in the fight against unsolicited email.

¹⁸ GBDe Paris Recommendations - Consumer Confidence, September 1999.

As noted above, an inherent difficulty in considering any new legislative initiative is the difficulty of defining unsolicited electronic communications coupled with constantly evolving technology and business models. While several jurisdictions have adopted varying legislative approaches, there has been little evidence of their effectiveness in actually curbing the global problem of unsolicited email. Many of these same legislative initiatives have had the negative effect of increasing the burden on and costs of legitimate commercial email users.

There are other potential pitfalls to consider before introducing any new legislative initiative. For example, legislation can be non-effective and even harmful if it pushes unsolicited emailers offshore where it is more difficult to enforce, thereby increasing the importance of harmonized legislation around the world. There is the possibility of unintentionally regulating not only free speech, but also individual consumer emails resulting in consumers inadvertently losing control of their email boxes. Furthermore, it is possible that industry will give up on best practices if they are penalized by legislation. Finally, consumer confidence in government's ability to provide protection could be undermined by the introduction of ineffective legislation.

5. International Cooperation

It is widely agreed that unsolicited email or spam is a global problem given the interconnected nature of the Internet. That problem is compounded by the fact that domestic legislation traditionally varies from country to country and by its very nature is applied to organizations operating within a particular jurisdiction. Therefore, international cooperation is needed at all levels and among all participants.

For example, in an effort to focus the discussion, consumer groups can increasingly come together to express their views on key Internet issues such as spam and extend their discussions on such issues to business and governments around the world. Self-regulatory measures adopted by

certain industries, e.g. the online marketing industry, are by default international and their implementation should not await the harmonization of national laws. In order to increase the effectiveness of the various legal solutions and to avoid the creation of spam havens, governments can collaborate to apply pressure to those "offshore" territories where there is a general lack of domestic consumer legislation and encourage international cooperation on enforcement.

Recommendations for Industry

Internet Service Providers

- **Adoption of voluntary practices**

Some of the following practices are widely used today while others are being considered as the negative impacts of unsolicited email increase¹⁹:

- establish, use and strictly enforce service agreements and acceptable use policies (AUPs) to prohibit the use of the service for sending unsolicited email;
- work with other ISPs both domestically and internationally to improve and harmonize practices and policies;
- limit the number of emails sent per day per IP address or email account as a condition of service;
- develop appropriate internal practices, recognizing the differences between individual and business customers; collect accurate customer data; adopt business practices that decrease opportunities for unsolicited emailers (e.g. limit number of accounts opened under the same name, credit card, etc.); proactively identify and terminate users who are likely unsolicited emailers while respecting privacy principles (e.g. quarantine suspect messages, have a threshold test, investigate and terminate);
- properly configure network services to decrease or eliminate the chance of being

¹⁹ Similar voluntary measures have been recommended in the GBDe Brussels Recommendations – Combating Harmful Internet Content – October 2002.

exploited by a sender of unsolicited email both outside and inside the network;

- establish hotlines, email contact points or other methods to lodge complaints;
- share contact and escalation procedures with other ISPs, both domestically and internationally, in an attempt to provide an agreed upon method to notify an ISP prior to blocking traffic from its domain with an explanation of the reason for the impending block and what may be done to avoid it; an industry association may be able to act as a point of first contact in these instances;
- agree to work closely with those affected to ensure a speedy resolution of wrongful blocking;
- use reputable external blacklist sites to filter out unsolicited email; and
- operate an internal blacklist of known unsolicited emailers whose mail should be blocked from customer in-boxes; depending on applicable legislation and fair information practices, there may be opportunities to share such information with other ISPs.

- **Cooperation with law enforcement**

ISPs and affected businesses should seek increased opportunities to cooperate with law enforcement, e.g. business can bring forth to law enforcement the best cases for prosecution.

- **Establishment of approved sender lists**

A key component of the self-regulatory approach could be the establishment of approved lists of email senders who meet agreed industry practices. Such an approach encourages continued self-regulation and increases consumer confidence in online marketing. There are already "white lists" in use by some ISPs but the aim would be to replace these with a transparent and publicly available industry-wide list or lists. The existence of an internationally approved sender list would help ISPs fine tune their unsolicited email strategies and may one day be used in combination with positive filtering at the recipient level.

- **Encouragement for ID programs, digital signatures and trusted digital certificates**

There are already a number of industry groups collaborating on enhancing the standards required for identifying, authenticating and authorizing subscriber requests for digital certificates to be used over the Internet. However, several major issues affecting the acceptance, use and comparability of digital certificates must be resolved, including levels of assurance assigned to certificates; required identification, authentication and authorization procedures; consistent application of standards and accreditation of Certifying Authorities (CAs)²⁰. Within the context of the unsolicited email issue, some of these remedies and trusted seals may have application for a wider range of digital communications beyond those of a transactional nature. Eventually, it may be that meeting such requirements becomes part of established industry practices.

- **Coordinated industry effort to decrease abuse of the network**

Open mail servers, once a hallmark of the interconnected and open network architecture of the Internet, have become a serious problem worldwide because they are easily hijacked by unsolicited emailers. This means that any party can identify an open server and use it to send out bulk unsolicited email to another company's email server. Even though the problem of badly configured mail servers is not likely to be totally eliminated, a coordinated effort by ISPs to identify, block, reconfigure or shutdown open relay mail services would undoubtedly be an efficient use of industry resources.

- **Agreed filtering strategies by ISPs**

Over time filtering should increasingly move towards the recipient who is in a better position to determine what may or may not be unsolicited email. However, until a multilateral approach is proven to be effective in substantially decreasing the amount of unsolicited email, ISPs will have

²⁰ GBDe Tokyo Recommendations, Cyber Security, September 2001

to continue to filter and block unsolicited emails by using various means available from outside lists to internally generated lists and methods. This practice will continue to be governed by contract and the language contained in AUPs and terms of service. However, one of the problems in developing effective blocking mechanisms is the eradication of legitimate email along with unsolicited email. There is a need for ISPs, perhaps coordinated by the largest global commercial providers, to cooperate to develop agreed filtering and technological solutions at the ISP level.

Commercial Users of Email

- **Adoption of voluntary practices**

The following are some of the practices, depending on the context, that have been voluntarily adopted to varying degrees by commercial users of email:

- develop and implement appropriate practices regarding the collection, use and disclosure of email addresses consistent with widely accepted fair information practices, and applicable privacy legislation, and ensure such practices are adequately promoted;
- employ different approaches depending on whether or not there is an existing commercial relationship with a preference for the use of opt-in where there is no pre-existing commercial relationship;
- consider the use of clear and conspicuous language in the subject line to identify email as commercial solicitation;
- provide a clear and easy “opt-out” of receiving future emails;
- maintain accurate and up-to-date email lists and “do not send” lists;
- when using a 3rd party email list, consider asking to see the consent language that was used to determine whether it was clear and easy to understand, whether there is an ongoing ability to opt-out, etc.; and
- when using a 3rd party email list, consider including a reminder in the first email to the individual as to how you obtained his/her email address.

- **Development of internationally acceptable codes of practice and acceptable standards**

As part of the objective of clearly defining and separating unsolicited email from legitimate business communications, direct marketing associations and other relevant bodies should develop, sign-up to and promulgate industry codes of conduct. The basis for guidelines are already in existence and it may be a case of fine-tuning, repackaging and promoting acceptable industry practices with relation to unsolicited email. These codes of practice should be international in scope and comply with the requirements of multiple jurisdictions. Making it harder to get email addresses will also go a long way to decreasing the level of unsolicited email and increasing consumer trust.

Recommendations to Government

Governments internationally have an important role to play in combating the rapidly growing problem of unsolicited email. Governments should partner closely with industry and consumer groups in developing an international strategy.

Enforcement

Governments should encourage enforcement agencies to adopt more aggressive interpretation, application and enforcement of existing criminal and consumer protection laws. The enforcement of existing laws, both domestically and internationally, would go a long way to combating the problem of unsolicited email and would send a message that governments around the world are serious about their role in combating unsolicited email.

International coordination and cooperation

Governments should seek the opportunity to develop an international policy framework by collaborating on coordinated unsolicited email reduction strategies. Despite being closely

linked to privacy, a more productive approach to the international dimension of the unsolicited email problem as defined above may be to consider it within the wider issue of cyber security.

Within this context responses may include:

- **Development of information sharing mechanisms between and within the private sector and government and legislative protection for this process**

The sharing of timely information on illegal Internet activity is a crucial part of tracking perpetrator and bringing them to justice. However, information-sharing mechanisms among industry for these specific purposes should be consistent with antitrust rules (and may need an explicit response from authorities). In addition, the information channels between industry and government for the same purpose must be protected by appropriate safeguards regarding privacy, data protection and data retention. The considerations are equally applicable to information sharing on cyber security issues and it may be more efficient to deal with both in similar terms.

- **Agreed international enforcement procedures for cross-border fraud**

The borderless nature of the Internet makes cross-border cooperation essential. The effect of legislation in some jurisdictions and the lack thereof in others will inevitably result in migration of spam activities to countries with less stringent legislation and the creation of spam havens. Governments need to ensure that there is adequate cooperation between enforcement agencies internationally relating to pursuit, prosecution and possible extradition of offenders.

- **Development of a global list of known unsolicited emailers available from appropriate government agencies and subject to due process and independent review**

There is considerable debate over the use of so-called "blacklists" of unsolicited emailers. These are generally managed and maintained by private individuals or organizations without sufficient transparency, independent review, privacy considerations or access to due process. However, a recognized and respected worldwide "blacklist" could provide a useful tool for ISPs in their attempts to reduce the volume of unsolicited email. Such an effort should also include either a mechanism to allow a party that has been wrongfully accused to be removed from the list or a mechanism whereby a notice is sent to the accused with an opportunity to respond prior to being placed on the list.

Legislation

Where enforcement of existing laws is not adequate, the introduction of new legislative initiatives may be required. However, it may be that no new Internet-specific legislation is required, but rather that existing legislation is amended to ensure its application to the online environment and the problems associated with unsolicited email (e.g. legislation and rules regarding fraud, advertising, trespass, etc.).

Governments should consider adopting a harmonized international legislative framework that:

- provides for redress through the imposition of strong criminal penalties and, where appropriate, private rights of action;
- clarifies what is illegal by defining what is an unfair, deceptive or misleading practice (e.g. falsification of sender and mail headers); and
- clearly defines fraudulent activities (e.g. hacking into accounts, open relay abuse, opening of multiple accounts, false registration of information for email addresses and domain names).

Governments should also consider the possibility of targeting the entity that hired the emailer and is benefiting from the unsolicited email since it is difficult in many cases to trace the more serious unsolicited emailers. Most unsolicited email is trying to convince a consumer to purchase something and so there is

potentially an ability to get at that merchant or marketer. Governments should consider:

- what type of liability would be appropriate under these circumstances; and
- what type of proof or causal link to the emailer is required to trigger such liability.

Education and Awareness

In accordance with a truly cooperative approach, government, business and consumer groups should combine forces to develop an international consumer education campaign.

Consumers should be viewed as part of the solution, not part of the problem. This will require new ways of educating and empowering consumers which could involve:

- provision of technical remedies including filtering technology to consumers;
- development of user guides and self-protecting Internet behavior; and
- understanding of rights, reporting and available remedies.