Draft WGIG Issues Paper on Spam

This paper is a 'draft working paper' reflecting the preliminary findings of the drafting team. It has been subject to review by all WGIG members, but it does not necessarily present a consensus position nor does it contain agreed language accepted by every member. The purpose of this draft is to provide a basis for the ongoing work of the group. It is therefore not to be seen as a chapter of the final WGIG report, but rather as raw material that will be used when drafting the report. This draft working paper has been published on the WGIG website for public comment, so it will evolve, taking into account input from governments and stakeholders.

1. Issue

Spam directly engages a very wide range of stakeholders that includes individual consumers, all organizations of whatever size in the private and public sectors that are Internet users, network operators and Internet Service Providers (ISPs), suppliers of Internet security products and services, commercial e-mail marketers, entities and organizations that commission spamming campaigns, a variety of government policy departments, regulatory authorities and enforcement agencies at the national level, and various intergovernmental and other international organizations at the regional and global levels.

Given the range of stakeholders engaged in the debate about spam and the diversity of their interests, it is perhaps not surprising that there is not at present an international consensus on the definition of spam, the specific governance issues it raises, or the most appropriate methods of resolving these issues.

Some stakeholders define spam broadly to include all unsolicited bulk commercial e-mail sent for direct marketing purposes or, more colloquially, as ‘electronic junk mail’. By this broad definition it is estimated that considerably more than half the e-mail sent today is spam.

Other stakeholders define spam more narrowly as commercial e-mails that are fraudulent, malicious, or misleading. In many cases, such e-mails violate national laws. Although it was originally confined to e-mail services and directed at consumers and users that used wireline technologies to access the Internet, spam is now spreading to other kinds of networks and services, including cellular telephone networks, weblogs, and instant messaging services in both wireline and wireless environments (where it is known as ‘spim’).

Although wireless spam and spim raise somewhat different issues from conventional spam, because of differences that typically exist in the design, operation, regulation and tariffing of services on these different kinds of networks, spam raises similar general concerns in all network and service environments.

From this broad perspective, spam raises a number of different kinds of governance issues.

- Spam can be annoying or offensive to consumers and imposes various additional costs, especially on individuals who access the network through pay-per-use or low bandwidth connections, thereby hampering the development of Internet access.

- Spam imposes significant costs on organizations in the private, public and not-for-profit sectors, whose employees may spend substantial amounts of work time sorting through e-mail messages to determine which are legitimately related to their work, and in deleting the rest.

- Spam also imposes significant costs on Internet Service Providers (ISPs) and other network operators, since it requires investment in a range of tools that are needed to counter spam, including anti-spam technologies (e.g. filtering technologies), server and transmission capacity, human resources, and anti-spam information sharing, cooperation, and regulatory structures. This is a particularly important concern in developing countries.
- Spam provides a cover for spreading viruses, worms, trojans, spyware, etc., which typically are sent as attachments to e-mail messages, which may cause harm to individual consumers and user organizations, as well as to network operators and service providers.
- As well causing inconvenience and reducing the utility of the Internet for consumers and users, spam may violate national law – e.g. if it constitutes an invasion of privacy (e.g. spyware), leads to malicious attacks on their personal property (e.g. viruses), or results in the unauthorized use of this property, possibly for illegal purposes (e.g. zombie networks).
- Spam also provides a cover for other forms of cyber crime, such as identity theft through "phishing" and other forms of online fraud, which cause harm to individual consumers and impose costs on corporations (e.g. in the financial services sector), and government agencies (e.g. that issue licences).

For all these reasons, there is growing concern that if spam is not controlled, it will constitute a serious impediment to Internet use for consumers and users, and a significant roadblock to the development of e-commerce, e-government, and online public services, thereby reducing the "social value" of the Internet. This is of particular concern to government policy-makers in developed and developing countries, although the specific concerns it presents may vary according to the level of technological and economic development within a country.

At the same time, it is also generally recognized that commercial e-mail which does not raise the kinds of issues listed above has a legitimate place in the development of e-commerce and the e-economy, and that measures to control spam must distinguish between acceptable and unacceptable commercial e-mail practices. This is of particular concern to businesses in both developed and developing countries, which see the new commercial opportunities made possible by e-mail and want to avoid being .subjected to overly onerous laws and regulations.

In this regard, commercial e-mail may be seen as a 'two-edged sword' by small and medium-sized enterprises (SMEs) in developing countries. On the one hand, it offers an opportunity to market their products and services internationally, and to participate in global e-commerce. On the other hand, the anti-spam laws and regulations being developed and implemented in other countries may create uncertainty and add to the cost and complexity of business operations.

The following kinds of factors can be used to distinguish between acceptable and unacceptable commercial e-mail practices:

- consumer and user consent;
- e-mail intent;
- mechanisms for authorizing or certifying information sources;
- honesty and transparency of communications;
- mechanisms for receiving and redressing consumer complaints;
- mechanisms to permit e-mail recipients to opt-out of receiving future communications;
- Spam originates in both developed and developing countries.

Whatever its origin, the negative effects of spam are magnified in developing countries because of factors such as:

- the slower access speeds generally available to consumers and users, and the relatively higher cost of access in relation to income;
- the relative lack of network and storage capacity available to network operators and Internet service providers, as well as of the financial, technical and knowledge resources needed to counter the negative effects of spam;
- the relative lack of legal, policy, regulatory and enforcement capacities in government.

2. Attribution to category / ies

As indicated in the Inventory, spam-related issues are principally attributable to the “access for all”, “stable and secure functioning of the Internet” and “multilingualism and content” categories.

However, as indicated in the preceding section, they also impact some of the “other issues for consideration”, particularly e-commerce, e-government, privacy, and exemption of ISPs for third party liability.

3. SWOT Analysis

There is at present no unified global system to control spam, although international cooperative action has begun among governments on a bilateral and multilateral basis, and, separately, among network operators and active Internet users.

At present, these activities are largely limited to the richest developed countries, many of which have spam control legislation and enforcement mechanisms in place. This could be considered a situation of strength since these countries account for well over half the spam produced in the world today. However, the limited involvement of other countries in international efforts to control spam could also be considered a significant weakness, given the ease with which spamming operations can be moved from one jurisdiction to another.

The opportunity presented by initiatives to control spam, which ranges from simple annoyance to outright criminal activity, is to benefit the development of e-commerce, e-government and the information society. Further innovation by business and others to develop even more effective network security and management applications could provide effective solutions in the future.

The threat, if effective governance is not developed, is to diminish the utility of the Internet for individual users, businesses, public and not-for-profit organizations, and to diminish or delay the realization of resulting benefits – up to and including making e-mail and other online communication systems practically unusable.

In the absence of effective governance, it is possible that a number of different, privately controlled, proprietary anti-spam solutions will emerge, thereby threatening the integrity of the Internet, its utility as a medium for the free flow of public and private correspondence, and the enjoyment of the rights associated with these different forms of communication.

4. Actors

Effective action to control spam requires the involvement of a wide range of actors, including:

- various policy departments, regulatory bodies and enforcement agencies of national governments;
- developers and suppliers of anti-spam technologies
- Internet service providers (ISPs);
- commercial e-mailers;
- civil society organizations that represent consumer and business interests;
- active end users, who monitor and report spam;
- intergovernmental and other international organizations involved in policy coordination and the development of technical standards.

5. Forums

As indicated in section 3, international cooperative action among governments is beginning on a bilateral and multilateral basis, with considerable consultation from non-governmental actors and in multi-stakeholder partnerships.

Examples of the former are the anti-spam enforcement agreements concluded by law enforcement agencies in the US, Australia and the UK.

Examples of the latter are:

- work that is under way in established international organizations – such as the OECD, which has developed an ‘Anti-Spam Toolkit’ and the ITU, which has established a database of anti-spam laws worldwide and competent enforcement authorities;
- initiatives such as “The London Action Plan on International Spam Enforcement Cooperation” that was developed in October 2004 by representatives of government agencies from 27 countries.

International business organizations such as the International Chamber of Commerce have developed policy recommendations and self-regulatory guidelines for use by their members and for consideration by governments and international organizations.

International standardization organizations, such as the Internet Engineering Task Force (IETF) and the ITU Standardization Sector (ITU-T) are working on standards that will assist in controlling spam, e.g. through authentication and certification of e-mail sources.

A large number of online forums and groups not only discuss spam, but are active in notifying spam cases, encouraging ISPs to take action, and developing anti-spam tools. The groups that develop tools usually take decisions about which criteria should be used to determine whether messages are spam, and which ISPs should be identified as spammers. However, it is then up to ISPs to chose whether to use these tools and act on this information, or not.

6. Governance mechanisms

The overall objective of the emerging system is to control spam in order to significantly reduce its negative impacts on consumers, businesses, public and not-for-profit organizations, while permitting legitimate commercial e-mail practices to develop as part of the emerging e-economy.

At the national level, this typically involves a “toolkit” approach that includes the following elements:

- campaigns to raise public awareness of potential abuses of e-mail and educate consumers and users in actions they can take to guard against the more pernicious effects of spam, such as viruses, identity theft and other forms of fraud;
- laws and regulations to define and prohibit illegitimate e-mail practices and proscribe penalties;
- enforcement mechanisms;
- industry self-regulation through the identification of best practices and the development of both codes of business conduct and information sharing processes for ISPs and commercial e-mailers;
- development of standards for authentication or certification of commercial e-mailers;
- development and customization of technical anti-spam tool kits to suit local languages.

At the international level, the bilateral and multilateral arrangements that have been developed to date typically involve:

- policy research, analysis and coordination;
- information sharing between public agencies responsible for anti-spam activities in different countries;
- information sharing between private sector organizations.

Among the global Internet community, a set of common rules, codified in the "netiquette" and similar documents, has been created throughout the years. Inter alia, these rules require ISPs:

- to have an online anti-spam helpdesk, reachable through the standard "abuse@<isp_domain>" e-mail address, that promptly deals with reported spam cases that involve the ISP and its users;
- to shut down the accounts of customers who use them to send spam;
- to require advertisers not to send mass e-mail to customers that did not grant their consent in advance;
- to require advertisers not to harvest e-mail addresses from websites, mailing lists, newsgroups, Whois databases and other online sources.

In some cases, these rules have been incorporated in national privacy or anti-spam laws and regulations. Otherwise, they have the status of recommended "best practices".

7. Adequacy measured against criteria / benchmarks set out in Declaration of Principles:

(a) multilateral

(b) transparent

(c) democratic

(d) capacity to address Internet governance in a coordinated manner

(e) multi-stakeholder approach

(f) other

It is still ‘early days’ to assess the adequacy of emerging spam international governance mechanisms against the criteria set out in the WSIS declaration.

One potentially strong point of these mechanisms has been the application at the international level of the multi-stakeholder approach which has been successfully adopted at the national level in a number of countries. However, it is not evident that the interests of civil society are as yet adequately represented at either governance level. In addition, developing country stakeholders from government, the private sector and civil society have yet to be effectively engaged. Although multilateral, the current arrangements are largely confined to the developed world.

A second potentially strong point has been the development of a coordinated, or ‘toolkit’ approach to controlling spam, which typically involves consumer awareness and education, industry self-regulation, legislation and enforcement. However, extending this approach from highly developed countries to the rest of the world will be a challenge, given the significant differences that exist among countries with respect to the development of their information and communications technology (ICT) infrastructures, Internet access, policy and regulatory capacity, legal frameworks and institutional structures.

A third potentially strong point has been the bottom-up, collaborative development of anti-spam governance tools over the Internet. However, even this process might not be sufficiently transparent and democratic to meet the WSIS standard, since it is usually very hard for non-technical people to participate in such informal, technically-oriented, developed country-based groups.