ITU WSIS Thematic Meeting on Countering Spam

CICG, Geneva, 7–9 July 2004

CHAIRMAN'S REPORT

Introduction

1. At the invitation of the ITU Secretary-General, an ITU WSIS thematic meeting on Countering Spam was held in Geneva, Switzerland, from 7 to 9 July 2004. The event was organized in the framework of the implementation of the Declaration of Principles and Action Plan adopted on 12 December 2003,[1] at the first phase of the World Summit on the Information Society[2] and in preparation for the Tunis phase of the WSIS, to be held November 16-18, 2005.

2. Dr. Robert Horton, Acting Chair, Australian Communications Authority chaired the Workshop.

3. The event web site at http://www.itu.int/spam/ provides links to the final agenda,[3] all background resources, presentations and written contributions,[4] and the participants list.[5]

4. Around 200 participants took part in the meeting, representing a range of government policy-makers and regulators, international and intergovernmental organizations, consumer groups, representatives of Internet service providers, ICT companies, academics, civil society organizations and others.

5. Mr. Yoshio Utsumi, ITU Secretary-General opened the meeting, welcoming all participants. He recalled the commitments made during the first phase of the WSIS to building a people-centred, inclusive and development-oriented information society in which information and communication technologies (ICTs) are accessible to all citizens of the world. In the WSIS declaration of principles, it is recognized that spam is "a significant and growing problem for users, networks and the Internet as a whole" and plan of action states that it is necessary to take "appropriate action on spam at national and international levels". New ways to cooperate in solving the problem of spam are therefore necessary, and this meeting could contribute to creating frameworks for international cooperation.

6. Dr. Horton argued that what is at stake is no less than the protection and preservation of the Internet as we know it, which is a resource critical to the developed world, but also to the developing one, where it constitutes a potential route to economic and social development. He noted that the organization of this meeting was very timely, given that is taking place at a moment when criminal forms of spam, such as "phishing" are rising. He invited the meeting to consider joining the commitment proposed by Bill Gates, the co-founder and chief software architect of Microsoft, to eliminate spam within two years.

---

[1] http://www.itu.int/wsis/documents/doc_multi-en-1161|1160.asp

[2] http://www.itu.int/wsis/

[3] http://www.itu.int/osg/spu/spam/meeting7-9-04/agenda.html

[4] http://www.itu.int/osg/spu/spam/background.html

[5] http://www.itu.int/osg/spu/spam/meeting7-9-04/Spam%20meeting%20registered%20participants%20-%20July%202004.pdf

7. In particular, Dr Horton suggested that there could be three main objectives to be achieved during the meeting:

- Recognition of the need for anti spam measures. This could include new legislation, which makes complementary anti-spam actions defensible and useful;
- Establishment of a loose network of information resources for legislators and practitioners considering spam legislation; and
- Development of a checklist or set of principles to assist new anti-spam efforts.

8. A comprehensive approach would be five-layered, including:

- Strong legislation,
- The development of technical measures,
- The establishment of industry partnerships, especially with Internet Service Providers, mobile carriers and direct marketing associations,
- The education of consumers and industry players about anti-spam measures and Internet security practices;
- International cooperation at the levels of government, industry, consumer, business and anti-spam groups, to allow a global and coordinated approach to the problem.

9. Dr. Horton concluded his approach stressing that the meeting will give the opportunity to develop international cooperation, giving ample opportunity for discussion of what is happening globally in terms of the problems, practices and approaches taken, improve contact with organizations from nations that have anti spam laws, should assist organizations from nations yet to, or currently considering, such actions, and develop initial principles which may assist or even underpin anti spam action.

10. Highlights of the meeting sessions are discussed below.

Sessions 1 & 2: The Scope of the Problem

11. Unsolicited commercial communications or spam, as it is more usually known, has grown into one of the major plagues affecting today's digital world. Over the last ten years, spam has grown to represent almost 80% of total e-mail traffic according to MessageLabs, with spammers sending hundreds of millions of messages per day. The estimated costs of spam to the global economy are approximately US$ 25 billion dollars per year. This is now causing significant financial costs and losses in productivity for service providers, businesses and end-users alike. With the growing dependence of users on the Internet and e-mail for their personal and professional communications, the phenomenon of spam is hampering the development of the information society by undermining user confidence and trust in online activities.

12. Although there is no universally agreed definition of spam, the term is commonly used to describe unsolicited electronic bulk communications over e-mail or mobile messaging (SMS, MMS), usually with the objective of marketing commercial products or services. While this description covers most kinds of spam, a recent and growing phenomenon is the use of spam to support fraudulent and criminal activities—including attempts to capture financial information (e.g. account numbers and passwords) by masquerading messages as originating from trusted companies ("brand-spoofing" or "phishing") – and as a vehicle to spread viruses and worms. On mobile networks, a particular problem is the sending of bulk unsolicited text messages with the aim of generating traffic to premium-rate numbers.

13. The term "spam" is currently used to cover two distinct types of activities:

- The first might be regarded as over-enthusiastic marketing, where the sender is obvious and there is no attempt to force messages onto networks or users that do not want to receive them.
- The second type is where the sender deliberately anonymises the message and tries to avoid all forms of detection and often buys facilities under false identities.

14. Depending on national interpretations, treating these two separate problems as one is highly dangerous because it allows the protection given to marketing and free speech to be extended to fraudulent activities.

This is clearly wrong. Spammers have proven highly creative in avoiding detection, including through the falsification of the origin of e-mail and randomization of content to bypass spam filters. The scale of the problem has continued to grow, despite the large number of technical solutions that have been developed to try to limit it. The number of networks that tolerate this type of activity is very small, but given the global nature of telecommunications, it is sufficient to do considerable damage. Spam is a major problem for developed countries, but perhaps is even worse for developing and least developed countries (LDCs), where, because of limited available Internet resources, many users rely on free web-based email services with limits on free storage, which are particularly targeted by spammers. The cost of receiving and deleting spam, over low-speed dial-up lines, represents a significant cost for developing countries and in essence means that the growing level of spam equates to a denial of service attack.

15. It was also highlighted that because of less effective security protection, computers on broadband networks are often compromised in order to hijack them to send spam (and commit other undesirable activities). In some cases, entire networks find their email is rejected by recipients because of their inability to deal with these problems. To address this, law enforcement in each country needs to deal with the problems at the source rather than impose this burden on the destination and developing countries need resources and training so that these networks can better manage the issues.

Session 3: Technical Solutions

16. Spam has become a widespread problem because it is financially profitable. This is due to the low start-up costs for spammers, and because the marginal cost of sending each new spam is estimated to be below 0.0005 USD. Furthermore, the basic Internet architecture for email (SMTP) allows emails to be sent anonymously.

17. The huge number of Internet users around the world (around 665 million at the start of 2003), the growing amount of daily email traffic (several billion per day), and the highly distributed nature of Internet infrastructure, makes any technical solution particularly complex. Filtering is a widely used practice, but there is a continual effort by spammers to bypass filters (e.g., keyword filters are avoided by spammers with cleverly misspelled words, adaptive filters are often circumvented by inserting legitimate tokens to confuse them, etc.)

18. Identification standards are being developed by a number of industry and standards groups, such as IETF through its MARID group, as well as by Internet Service Providers, which are trying to collaborate to limit the spread of spam. Although authentication systems are deemed to be a critical part of the solution, their implementation remains problematic, and the wide adoption of a standard authentication method seems far away. Furthermore, the cost of technical solutions, the level of technical support necessary and the need for continual updating, present cost issues for developing countries, their ISPs and their users.

19. This issue may be exacerbated by the fact that, at present, most of the technical work is done in developed countries. In particular, technical developers are often not familiar with conditions in developing and least developed countries. This suggests the need to reinforce capacity-building initiatives.

20. It was clear from discussion that there is no silver bullet to curb spam. Technical solutions can have the un-intended effect that spammers need to increase they volume of spam they send in order to ensure that a small proportion get through, but they have not yet deterred spammers. Technical solutions have to be combined with in a multi-track approach incorporating legislation, public education, industry self-regulation, standardization and international co-operation.

21. It might be appropriate to revisit some of the original design principles of the ITU-T X.400 standards to consider whether they could provide guidance for future developments, particularly with regard to lessons learned.

Session 4: Consumer Education and Awareness

22. This session identified a number of requirements and suggestions for action;

a) There is a need for consumer education on use of the Internet and the negative impact of Spam, Phishing and other nuisances. Information/education from ISPs, Carrier/Operators, Retailers, Consumer Bodies, Business Organizations, Governments and advertising campaigns will help;

b) Research illustrates a lack of consumer confidence regarding online marketing and email, which could have a critical impact on the Internet and its associated benefits – such as access to information, educational opportunities, legal marketing, email communication and online servicing by customers;

c) Data privacy issues are also an area of consumer concern (because of spam and fraud). There is a need to consider new ways to engender consumer confidence and offer consumer consent mechanisms;

d) Direct marketing has changed out of all recognition from off-the-page, postal direct mail, television and radio. A panelist suggested the new era needs to have constructs that place the consumer in control. With multi-media marketing, consumers now feel the need to know who has their data and how this data is being used. This is an important consideration, as many countries do not have separate Data Privacy legislation. There is a perception that new media make direct marketing more intrusive. Spam has great contributed to this perception. This challenge also links back to a) above;

e) The convergence of fixed and mobile networks and new services has strongly impacted upon spam. There are high costs to the Internet industry, businesses and consumers resulting from spam, phishing (and other forms of fraud) and the need for heightened security (viruses, spyware). Also concerns were voiced regarding protection of children having access to inappropriate services. Although software is available to block PC and mobile access, there is a crucial need for consumer education;

f) The overall conclusion from this session was that multiple actions are necessary to deal with spam, phishing and other fraud to make the Internet experience safe for consumers: these include, in parallel, technical solutions, consumer awareness and educational programmes, legislation and strong enforcement and international co-operation, including national legislation and Memoranda of Understandings (MoUs).

Session 5 & 6: Spam Legislation and Enforcement: A Cross-Border Issue

23. Legislation is a fundamental tool in the anti-spam battle. However, attention must be paid to enacting appropriate and efficient legislation in conjunction with appropriate funding for enforcement. A panelist argued that in many countries anti-spam laws could be defined as “sentiment laws”, i.e. laws that limit themselves to loathing spam, but which are not action-oriented, and do not effectively support legal action against spammers. The goals for legislation should be to decrease the cost of identifying and prosecuting spammers, increase the likelihood of obtaining successful prosecutions, and support effective ISP and operator action against spam. This should diminish the cost that society is expected to bear, and increase the benefits obtained by removing a spammer from the network.

24. To take concrete action against spam, and enact appropriate and effective laws, will require political will and commitment. Despite the enactment of spam legislation in recent years, with some exceptions, it does not yet seem to have had a significant impact on the volume of spam. Although legislation is in place in more than 30 countries, enforcement mechanisms seeminly need refinement, or are too complex to allow users and operators to take judicial action against spammers. However many of the laws are still being implemented, and enforcement mechanisms are experimental. Going forward, focusing on limited areas such as protecting children from being targeted by inappropriate content may be fruitful. Legislation such as this has been passed by at least a few US states.

25. Spam is not only growing in volume, but also changing in nature. Today a large part of spam messages involve fraudulent and deceptive content, and are therefore already illegal even in countries that do not have specific anti-spam laws, as they amount to fraud, theft, violation of private property, etc. The list of potential offences that spammers commit is indeed extensive. However, national laws, while potentially helpful, require strong, targeted enforcement in order to be effective. Given the fact that spam observes no national boundaries, and the cross-border nature of the Internet generally, it is essential that those who seek to enforce anti-spam laws cooperate with those in other nations to make anti-spam laws have a serious impact. Establishing rules to help create a jurisdictional nexus between senders and recipients is critical to enforce anti-spam laws.

26. Law enforcement officials taking on spam face a number of substantial challenges in getting their job done. First, there is little agreement across jurisdictions as to what anti-spam laws prohibit (for instance, opt-in v. opt-out). Disagreement remains even as to what spam is (for instance, must it be commercial to be prohibited?). Second, there is clearly widespread disregard for existing anti-spam laws (the "sense of impunity" among spammers). Violators today have substantial ability to evade prosecution, at least for a while. Third, nations wishing to cooperate have varying legal regimes and methods of enforcement from one to the next. These differences among prospective partners may present problems for the implementation of any enforcement-related MoUs or treaties. Other challenges include identifying spammers, obtaining evidence, recovering assets, sharing evidence, and preventing further misconduct.

27. There are rays of hope in terms of law enforcement and cross-border cooperation in the struggle against spam. French regulators have had success by seeking first to clean up the French market and by sharing information with other European colleagues. Regulators in the Republic of Korea have made progress through working in partnership with industry and others, including with the Australian Communications Authority through a bilateral agreement. Italy, besides its legal framework, has adopted a multi-faceted anti-spam regime, including technical, educational and law enforcement strategies. Japan has succeeded in reducing mobile spam by legislation and self-regulation. The United States, both before and since the CAN SPAM Act took effect, had successfully prosecuted more than 60 major spam cases and has handled thousands of consumer complaints. In many of these enforcement efforts, other countries have provided valuable information and cooperated in helping to bring the wrongdoers to justice. The private bar in the United States has also contributed to the fight against spam by bringing large civil actions against spammers over the past several years, in some cases even in the absence of specific anti-spam legislation. However, these early results have made a modest dent in the worst spamming activity. Enforcement is a long way from reversing the clear trend toward more, and more pernicious, spamming on a global level.

28. Law enforcement alone is not the solution; it should be regarded as one of several tools in the anti-spam toolkit. Most agreed that law enforcement should focus its efforts on the worst cases: fraud and other computer crimes. Some countries would like advice on how best to participate in the global anti-spam efforts and seek guidance. The session ended with a strong sense that there is indeed the energy and the determination among multiple players to collaborate in turning back the tide of spam. It is plain that there is an opportunity for leadership in this space.

29. Legislation is still not in place in developing countries though they share the common problem of spam, and of participation in spamming activities. For these countries, what is needed includes a set of international standards on acceptable ethics, the exchange of ideas and experiences, and development of best practices. Meetings such as this could be very helpful as they allow the exchange of ideas and experiences with a large number of countries, creating awareness on the possible anti-spam solutions. There is also a requirement for technical assistance in this area.

Sessions 7 & 8: Multilateral and Bilateral Cooperation

30. In these sessions, multilateral organizations (ITU, OECD, APEC), regional bodies (EU) and member states (Australia, UK, Canada, Republic of Korea, China and Brazil) presented a review of their initiatives to tackle spam and their views on possible future international cooperation. Since the society and culture of each country are different, it would be very difficult to employ the same anti-spam legislation everywhere. Nevertheless, sharing of information among different national authorities, and a cooperative approach to anti-spam laws enforcement is fundamental.

31. The opinion is that a global solution is needed, but there are a variety of possibilities. There are already many different international initiatives on countering spam (e.g., the OECD anti-spam toolkit, International Consumer Protection and Enforcement Network (ICPEN), APEC Consumer Guidelines, EU Network of Anti-Spam Enforcement Agencies, and the Australia/Korea MoU on the regulation of spam). Three new initiatives were announced during the meeting:

- The signing, on 2 July 2004, of an MoU on mutual enforcement on commercial email between enforcement agencies of Australia, UK and USA, which will include a meeting in London in October 2004;

- The establishment, on 8 July 2004, of an OECD Task Force on spam and the OECD's 2nd spam workshop to be held in Busan, Republic of Korea in early September 2004, in conjunction with ITU TELECOM Asia;
- The holding of a special session on spam at the ITU's Global Symposium for Regulators in December 2004.

32. It will be necessary to engage a larger number of countries, including developing countries, in cooperative action. One possible way of doing this would be by creating a multilateral MoU, building on some of the models that already exist. This proposal had been launched at the ITU's Global Symposium for Regulators in December 2003 and further discussed in a virtual teleconference. Brazil noted that spam is an Internet Governance issue and proposed that further discussion of an MoU should be organized in a forum in which all countries have an equal and meaningful possibility to participate in its elaboration, such as at ITU.

33. It is clear that there is some duplication between these different international initiatives, and there is a need to build upon the core competencies of the different agencies involved. ITU's core competencies that can be used in the fight against spam include:

- Public/private partnerships, through its unique membership structure of 189 Member States and more than 700 Sector Members;
- A leading managerial role in the organization of the World Summit on the Information Society;
- Standardization, including processes and data formats;
- Ongoing work with regulatory agencies, including through the Global Symposium for Regulators (GSR) and the G-REX global regulator's exchange service;
- User education and information sharing (through workshops, handbooks, tutorial material, databases, websites etc);
- Capacity building, especially through its centres of excellence.

34. There is urgency in tackling the matter of spam, but there is also a need for pragmatic steps towards cooperation, learning from current processes and nascent experiences, through an inclusive dialogue involving all actors and international organizations, which have a role and expertise in spam issues.

Session 9: Frameworks for International Action

35. Each of the rapporteurs provided brief reviews of their sessions. The chairman offered his personal observations, as recorded below. Comments from the floor noted that there was a great need for assistance for developing countries. Developed countries already have their forums, where they can cooperate, but developing economies depend on ITU. The Chairman noted that for every developing country present here, there were 20 countries that could not attend.

Personal observations of the chairman on the WSIS Thematic meeting on Countering Spam

36. This ITU meeting looking into the problem of spam reflected the urgency with which this problem needs to be dealt with: it has become a major annoyance and cost to Internet users and ICT industry alike, eroding trust in the information economy and with the more recent developments such as "phishing" and an increased fraudulent activity, the public confidence in the information platform could now be seriously threatened if remedial action is not taken.

37. Most speakers and participants seemed to agree that, as noted in the ITU background papers for the event, there is no 'silver bullet', or consensus emerging on the right way forward, as no one solution alone will curb spam. A multi-pronged approach to solving the problem, involving all stakeholders, is clearly necessary. The combination of technical solutions, user awareness, appropriate and balanced legislation followed up with measured enforcement, industry initiatives including those by the marketing community, and international cooperation, are seen as key elements. In addition, measures related to WHOIS data might be considered.

38. All actors—users, industry and governments—need to engage in a concerted effort, linking the mandates and expertise of various international organisations such as ITU, ICPEN, and the OECD, as well as the Internet Society, to support and progressively develop an international framework to combat this inherently global problem.

39. Countries could usefully continue to share experiences and best practice as they develop their own legislation and learn from those already in place. Several emerging international cooperative arrangements have been discussed, and a number of commentators identified a need for effective national enforcement arrangements, solid foundations to underpin possible future international frameworks.

40. There are some path-finding efforts in multilateral and bilateral cooperation through MoUs (e.g. Australia/Korea, and USA/UK/Australia), which should provide a valuable reference for what can be achieved and which could be potentially expanded in the future as other countries and their regulators develop their capabilities.

41. Further discussions between governments and industry, and practical measures, such as the proposed OECD anti-spam toolkit, the MoU on mutual enforcement and the discussion among regulators at the ITU Global Symposium for Regulators, should therefore all be encouraged. Upcoming events include the OECD workshop on 8-9 September in Busan, the enforcement workshop in London in October and the special session on spam at the GSR in December 2004.

42. Turning specifically to ITU, and what can be done as an action–oriented observation, given the diverse membership and valuable reach of ITU, together with its sensitivity to equity of treatment across its membership, it would seem valuable to re-focus in the short term on building a foundation for further cooperation in the combating of spam. At this point in time, the priority in developing cooperative legal solutions would seem to be establishing national laws and regulatory responsibilities as a first step in all countries. This would be by no means exclusive of exploring parallel technical solutions.

43. This would be a necessary preparation for a global regulatory foundation, and assistance in achieving this would be well appreciated by developing countries. With this foundation in place, a global MoU would then be feasible and more realistic. It would then provide a truly global solution to a global problem. Optimistically, a target of two years might be envisaged to reach that point, and by that time the back may then be broken with spam issues as we know them.

44. It is hoped that the observations in this report might inform a number of related activities within ITU: firstly, the General Secretariat and the potential to inform the WSIS preparatory process — consistent with the decision of ITU Council 2004, this report will be submitted to the ITU Council Working Group on WSIS. Secondly, the role which the ITU-D sector can play, through the GSR and G-REX, in assisting the immediate challenge to developing legislation, using models, experience and reference materials which might be used from other international efforts, together with a valuable survey of needs and capabilities which currently exist with spam matters. Finally, the ITU-T Sector might also be solicited to help in providing proper definitions and proposing technical solutions, in liaison with IETF, while benefiting from strategic consideration of technical spam matters in the meeting report and papers.

45. I would also encourage participants to provide ITU with a list of contacts dealing with spam issues in each national administration, and details of their current spam-related laws, to facilitate further dialogue within ITU and other international organisations, which have a role in the spam agenda. There should also be consideration of spam within the larger context of cybersecurity, as highlighted in the WSIS paragraphs that made reference to spam.

Finally, I would like to thank the ITU Secretary-General and all the involved ITU staff for their efficient and dedicated support for this event.

Dr Robert Horton, Acting Chair, Australian Communications Authority.

Chairman