ITU WSIS THEMATIC MEETING ON COUNTERING SPAM:

MULTILATERAL AND BILATERAL COOPERATION TO COMBAT SPAM

International Telecommunication Union

This paper has been prepared for the ITU World Summit on the Information Society (WSIS) thematic meeting on Countering Spam, organized under the ITU New Initiatives Programme by the Strategy and Policy Unit (SPU). The paper was written by Philippe Gérard, DG Information Society, European Commission, Bruxelles.

The meeting project is managed by Robert Shaw (Robert.shaw@itu.int) and Claudia Sarrocco (Claudia.sarrocco@itu.int) of the Strategy and Policy Unit (SPU) and the series is organized under the overall responsibility of Tim Kelly, Head, SPU. This and the other papers in the series are edited by Joanna Goodrick; see www.itu.int/ni.

Purpose and methodology

The present paper aims to describe what multilateral and bilateral cooperation could promote in the area of unsolicited commercial communications or 'spam'.

Sections are generally illustrated by corresponding actions initiated by the European Union. (A table annexed to this paper summarises the actions recently suggested by the European Commission to EU Member States, industry and consumers.)

The paper is not intended as an exhaustive overview of the current and planned multi- and bilateral cooperation initiatives, not least since many initiatives are works in progress at the time of writing this paper. (A summary overview of international initiatives is provided in the paper 'Spam in the Information Society: building frameworks for international cooperation' prepared by the ITU secretariat[1].)

The sessions at the WSIS 'Thematic meeting on countering spam' of 7-9 July 2004 provide an opportunity for representatives from various regions in the world to update participants on ongoing multilateral and bilateral cooperation efforts.

[1] See in particular session 4 'International initiatives in the field of spam. The paper is available at: http://www.itu.int/osg/spu/spam/background.html

Background

Unsolicited commercial communications, typically by e-mail, otherwise known as 'spam' have reached worrying proportions. More than 60 percent of global e-mail traffic is now estimated to be spam according to experts, although with regional variations[2]. What is even more worrying is the rate of growth: in 2001 the figure was 'only' 7 percent according to the same sources.

Spam is a problem for many reasons, e.g. privacy, deception of consumers, protection of minors and human dignity, extra costs for businesses, lost productivity. Spam is also increasingly used in combination with, or as a vehicle for viruses. More generally, it undermines consumer confidence, which is a prerequisite for the success of electronic commerce, electronic services and, indeed, for the development of the Information Society.

A crucial role for multilateral and bilateral cooperation

Appropriate action on spam, at both national and international levels, was clearly identified in the Declaration of Principles and Action Plan adopted at World Summit on the Information Society (first phase, Geneva, December 2003), as part of a wider effort aimed at building confidence and security in the use of ICTs.

A multi-faceted approach is generally considered as the best way to combat spam. Adopting effective legislation is a necessary step in this approach, although it is only part of the answer. Also important are: effective enforcement by competent authorities, technical and self-regulatory solutions by industry, and consumer awareness.

> In its January 2004 Communication on unsolicited commercial communications or 'spam', the European Commission, after consultation with interested stakeholders, identified a range of actions to complement the new rules against spam[3]. These actions indeed cover: effective enforcement, technical, self-regulatory solutions, and greater awareness. Generally speaking, the strategy is endorsed by EU Member States[4].

For reasons of efficiency, however, ongoing 'anti-spam' efforts made in various regions of the world, including the European Union must be replicated by similar efforts at the international level, by governments, businesses, and consumers. This international dimension is indeed crucial, since much spam comes from outside national borders in most countries, often originating in a limited number of specific countries.

The present paper briefly sets out the various types of actions that international cooperation could seek to promote. In brief, successful international 'anti-spam' cooperation could address at least the following facets:

- An effective 'anti-spam' law in all countries;

---

[2] See e.g. Brightmail, 2004.

[3] This document, as well as many other EU documents quoted in the present paper, can be accessed via the following URL address: http://europa.eu.int/information_society/topics/ecomm/highlights/current_spotlights/spam/index_en.htm

[4] See Council Conclusions 'on unsolicited communications for direct marketing purposes or 'spam', adopted on 8 March 2004.

- Cross-border cooperation on enforcement in specific cases;
- Self-regulatory solutions by market players e.g. on contractual and marketing practices;
- Technical solutions to manage or reduce spam, like filtering and other security features;
- Greater consumer awareness about, e.g., how to minimise spam and how to react to spam and complain.

While the two first facets relate to activities which are mainly for States and competent authorities to undertake, it is also important to promote internationally self-regulatory solutions, technical solutions, and consumer awareness. Only if integrated, coordinated action is pursued by all players, from governments, through businesses, to users and consumers, can individual actions be effective.

1. Promoting effective legislation in every country

First of all, international cooperation should seek to promote effective legislation against spam.

Adopting effective legislation is a first, necessary step in combating spam. While legislation may not be sufficient, it is the minimum necessary to cope with spam, to define rights and obligations, and thereby ensure as much legal certainty as possible.

Effective legislation may not preclude some diversity in the regulatory approaches taken in various regions. However, account should be taken as much as possible of existing approaches since international cooperation is needed to combat such a borderless issue as spam.

> As an illustration, in July 2002, the EU adopted Directive 2002/58/EC on Privacy and Electronic Communications, that introduced throughout the EU the principle of consent-based marketing for electronic mail (including mobile SMS or MMS messages), and complementary safeguards for consumers.
>
> The three basic rules under the new EU regime can be described as follows:
>
> - Rule No 1: E-mail marketing is subject to prior consent of subscribers. There is a limited exception for e-mails (or SMS) sent to existing customers by the same person on its similar services or products. This regime applies to subscribers who are natural persons, but Member States can choose to extend it to legal persons.
>
> - Rule No 2: Disguising or concealing the identity of the sender on whose behalf the communication is made is illegal
>
> - Rule No 3: All e-mails must include a valid return address where to opt-out
>
> Other existing EU provisions not exclusively targeting spam are also important, such as those banning disguised advertising, email harvesting, fraudulent or deceptive spam, hacking and identity theft. [5]

[5] References can be found in the mentioned Communication on unsolicited commercial communications or ‘spam’.

Effective legislation also implies that countries have the necessary investigation and prosecution powers. This includes having the appropriate tools to deal with spam cases such as appropriate remedies and penalties, complaints mechanisms, monitoring, etc.

Importantly, legislating effectively means that national authorities are granted the powers to effectively co-operate with counterparts in third countries (see section 2). Since spam is a global problem, competent authorities must be able to work across national borders

2. Promoting international cooperation on enforcement

Secondly, in view of the global nature of spam, international cooperation on enforcement is essential in order to ensure the effectiveness of anti-spam rules. In other words, it must be possible to trace back spamming activities and prosecute spammers, regardless of national borders.

> The EU rules apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the European Union (and the EEA). The rules are applicable to all unsolicited commercial communications received on and sent from public networks in the EU (and EEA). This means that messages originating in third countries must also comply with EU rules, as must messages originating in the EU and sent to addressees in third countries.
>
> The actual enforcement of the rule with regard to messages originating in third countries will clearly be more complicated than for messages from inside the EU. Hence the importance of international cooperation, since much spam comes from outside the EU.

As a pre-requisite, national legislation could facilitate information sharing and mutual assistance between competent authorities in different countries. Appropriate bilateral and/or multilateral cooperation would enable appropriate information sharing and mutual assistance on specific spam cases.

The choice of the international instrument(s) to do this may depend on various factors. However, all organisations can in any event promote such cooperation on enforcement within the limits of their competence.

Certain countries, including some EU Member States, have concluded cooperation agreements (e.g. Memoranda of Understanding) to facilitate such cooperation. These documents generally call upon participating parties to produce their 'best efforts' to cooperate with each other on issues such as building evidence, user education, new spamming activities, training, etc.

> Bilateral cooperation is promoted in the EU. Some EU countries have already signed Memorandums of Understanding with third countries covering at least some forms of unsolicited commercial communications or 'spam' prohibited in the EU (see the MoU recently agreed between various competent authorities in the UK, USA and Australia, focusing on certain). [6]

[6] This Memorandum of Understanding (MoU) is available at e.g. :
http://www.dti.gov.uk/industries/ecommunications under the Directive on Privacy and Electronic

> Since December 2003, competent authorities in the EU meet regularly to exchange information and best practices on issues related to enforcement. Appropriate contact details are been exchanged and an informal online network of competent authorities has been set up. This work with national authorities will continue throughout 2004.

At the multilateral level, some countries already participate actively in international discussions (e.g. ITU, OECD, APEC, EU), where work on spam has started. Active participation in this work of all countries with originators and recipients of spam is encouraged.

Ann OECD workshop on spam in February 2004 (hosted by the European Commission) had as its objectives to understand better the problems created by spam and to contribute to solutions at the international level. Concrete follow-up actions at OECD level are building on the results of the workshop. A second OECD workshop will be held in Korea in September 2004 that will explain the multi-facets, 'toolkit' approach taken by OECD, and will investigate in particular one such facet i.e. the technical solutions to spam.

At the UN level, the Declaration of the World Summit on the Information Society (Geneva, 10-12 December 2003) and the associated Action Plan stress that spam should be dealt with at appropriate national and international levels. The European Commission services are discussing with Member States follow-up actions to these two initiatives.

3. Promoting self-regulation by industry

Thirdly, industry - service providers, direct marketeers, software makers - can do a lot to combat spam by adapting their practices. This should be promoted across the globe, in particular since many companies operate on a multinational basis.

This concerns not only contractual practices (e.g. adaptation of terms and conditions for use of servers) but also marketing practices.

Self-regulatory tools (e.g. codes of conducts) should be encouraged and systematically improved with experience. Industry should also be encouraged to share their expertise and best practices, both across industry branches (e.g. direct marketeers with ISPs, and those players with software manufacturers), and across countries and regions in the world.

Improved cooperation on enforcement between industry and enforcement authorities should also be promoted, in particular to trace spammers and provide evidence that will be used to build investigation and prosecution.

> The European Commission favours self-regulatory solutions, building on existing rules, as well as cooperation between public authorities and businesses. Under certain circumstances EU-wide codes of conduct can be approved at EU level. Discussions are also ongoing at both EU and national level on cooperation in relation to enforcement (e.g. evidence building, etc).

Communications. The signatories to the MoU are the Federal Trade Commission (FTC) in the United States, the Australian Communications Authority (ACA) and the Australian Competition and Consumer Commission (ACCC) in Australia and the Department of Trade and Industry (DTI), the Information commissioner (ICO) and the Office of Fair Trading (OFT) in the United Kingdom.

4. Promoting technical solutions

Fourthly, industry, research bodies and particularly the Internet community need to continue to develop technical anti-spam solutions. This work should be promoted internationally.

Collaboration is required across sectors of industry (internet and email service providers, network operators (carriers), software developers) on anti-spam technologies.

This is both a short-term and a longer term issue. Security measures must be promoted (e.g., on filtering, open servers, open proxies). Filtering or software services as a basic customer service should also be recommended. Current developments identification can also contribute to better security, and hence to less spam.

Other adaptations also need to be considered in the longer term. Research in the economics of the technology used is also important to understand the business models for spamming and to consider how to create economic disincentives to spamming. Monitoring the trends and developments of spam is also necessary.

> While technical solutions are mainly for industry to develop, the European Commission has suggested in its January Communication some elements for the further development of technical solutions. Notably, filtering companies have been invited to cooperate with other interested parties to develop techniques recognising marketing e-mails corresponding to accepted marketing practices. Also, owners of mail servers and proxies have been invited to properly secure these tools. Also, under the successor of the Safer Internet Action Plan, more financial resources should be made available to fund anti-spam efforts.

5. Promoting awareness and education

Finally, awareness and education of consumers and businesses are also central. Consumers in particular must be in a position to know:

- what the rules of the game are;
- how to limit his or her exposure to spam;
- what filtering or basic security measures can be taken to minimise spam;
- where to complain when confronted with spam.

> In the EU, Member States and competent authorities have invited to launch or support campaigns in early 2004. All parties should play their role in awareness raising activities, from Member States and competent authorities, through businesses, to consumers/user associations.

6. CONCLUSION

The above remarks give a general overview of the kind of multifaceted approach that could be taken to combat spam effectively, as well as the nature of the international cooperation that will be required, on a medium to longer-term basis.

The WSIS 'Thematic Meeting on Countering Spam' could be used to discuss and build consensus on one or more specific cooperation initiatives, based on activities developing in different regions of the world including some of the EU actions outlined above.

> As an example, it was pointed out at the recent 'virtual' conference on regulatory cooperation on Spam on 30 March 2004, hosted by the G-Rex network of the ITU that cooperative actions among regulators might include[7]:
>
> - Establishment of working links amongst regulators;
> - Sharing technical expertise, commercial intelligence, educational strategies and
> - material;
> - For joint enforcement, use of existing and cooperative international fora such as the ITU, OECD, EU and others;
> - Support for technical enforcement partnerships;
> - Enforcement and regulatory policy co-development; and
> - Comparison and promotion of publicity messages.

The choice of any specific initiative would naturally depend on elements such as its objective(s) (e.g. promoting enforcement, promoting awareness), its participants (e.g. multilateral, bilateral, regional, and local) and its addressees (e.g. public, public-private, private).

***

[7] Report available at: http://www.itu.int/ITU-D/treg/Events/Seminars/Virtual-events/Spam/index.html

ANNEX – EXCERPT FROM THE COMMUNICATION OF THE EUROPEAN COMMISSION ON UNSOLICITED COMMERCIAL COMMUNICATIONS OR 'SPAM' (COM (2004)28, 22 JANUARY 2004)

TABLE OF ACTIONS IDENTIFIED IN THE COMMUNICATION

The table below summarises the actions identified in the Communication. For the purpose of this table, Commission/Commission services actions have been listed separately. As indicated above, actions are related to each other in several ways and should be implemented as much as possible in parallel and in an integrated fashion.

I – Effective implementation and enforcement by Member States and competent authorities

As a prerequisite, Member States should transpose the Directive on Privacy and Electronic Communications, in particular the provisions on unsolicited communications, without any further delay.

Member States and competent authorities should assess the effectiveness of their enforcement mechanisms in terms of remedies and penalties, complaint mechanisms, intra-EU co-operation and co-operation with third countries and monitoring. Member States should also develop national strategies to ensure co-operation between DPAs, CPAs and NRAs, and to avoid overlap and duplication between the authorities.

Member States and competent authorities should in particular:

(a) Effective remedies and penalties

- create adequate possibilities for victims to claim damages and provide for real sanctions, including financial and criminal penalties where appropriate;
- in Member States with no administrative remedies, consider the creation of such administrative remedies to enforce the new rules;
- equip competent authorities with the required investigation and enforcement powers;

(b) Complaints mechanisms

- establish adequate complaint mechanisms, including dedicated e-mailboxes for users to complain;
- co-ordinate the action of the various competent national authorities involved;

(c) Cross-border complaints and co-operation on enforcement inside the EU

- use existing, or if needed create, a liaison mechanism by which national authorities can cooperate in pursuit of cross-border enforcement (information exchange, mutual assistance) inside the EU. In this context, regarding fraudulent and deceptive spam in particular, the Council and the Parliament are urged to agree as quickly as possible on the proposed Regulation on consumer protection co-operation and investigate how far the Directive on Privacy and Electronic Communications should be added to the scope of the Regulation;

(d) Co-operation with third countries

- actively participate in multilateral forums (e.g. OECD) to elaborate solutions at the international level;
- reinforce, or engage in bilateral co-operation with third countries,
- investigate with the Commission what specific initiative it could take to facilitate international co-operation;
- cooperate with the private sector to trace back spammers subject to the appropriate legal safeguards.

(e) Monitoring

- ensure that they have the information and statistics needed to target their enforcement efforts, in co-operation with industry where appropriate and taking into account the ongoing OECD work on measurement.

II – Self-regulatory and technical actions by industry

Market players (e.g. ISPs, ESPs, mobile operators, software companies, direct marketeers) should seek to turn the opt-in regime into a day-to day practice, in co-operation with consumer/user associations and competent authorities whenever appropriate, and in particular:

(a) Self-regulatory actions

- assess, and if needed adapt, service providers' (ISPs, ESPs, mobile operators) contractual practices towards subscribers and towards business partners; provide information on filtering and possibly provide filtering software or services as optional customer service
- adapt direct marketing practices to the opt-in regime, and possibly agree specific, legally compliant methods to collect personal data (e.g., 'double' or 'confirmed' opt-in systems)
- develop and disseminate effective codes of practices (e.g. the FEDMA initiative) which are opt-in compliant, in co-operation with the Article 29 Data Protection Working Party or competent national authorities where appropriate
- consider the use of labels for opt-in compliant e-mails and databases to help users (and filters) recognise them, in line with the Directive on Electronic Commerce
- use, or create if needed, effective self-regulatory complaints mechanisms and alternative dispute resolution mechanisms (ADR) building on existing initiatives whenever possible (e.g. EEJ-NET).

(b) Technical actions

- (Filtering software providers) must ensure that their filtering systems are compatible with the opt-in regime and other requirements of EU law, including requirements linked to the confidentiality of communications; Member States and competent authorities are invited to clarify the legal conditions in their country under which different types of filtering software can operate, including privacy requirements
- (Filtering software providers) need to take into account the consequences for users of 'false positives', 'false negatives', certain forms of content-based filtering, and the possible associated liability issues. Users should be given the opportunity to manage the way in which incoming spam is handled, according to individual needs
- (Filtering software providers) should cooperate with interested parties to develop techniques recognising legitimate marketing e-mails legitimate (i.e. corresponding to accepted marketing practices under Community law) e.g. labels
- (Providers of e-mail services, and of mobile services where appropriate) should offer filtering facilities or services to their customers as an option available on request, as well as information on third party filtering services and products available to end-users
- (Owners of mail servers) should make sure that their servers are properly secured so that those servers are not in 'open relay' mode (if this is not justified). The same applies to open proxies.

III – Awareness actions by Member States, industry and consumer/user associations

Member States and competent authorities not yet doing so are invited to launch or support campaigns in early 2004.

All parties, from Member States and competent authorities, through businesses industry, to consumer and/or user associations should be active in practical information campaigns on prevention, acceptable marketing practices, and on technical and legal solutions available to users, and in particular:

- target actions at a) companies involved in or making use of direct marketing, b) consumers who subscribe to e-mail services, including SMS services and c) providers of e-mail services, including providers of mobile services.
- provide businesses and/or consumers with:
- a basic but widespread understanding of the new rules and on their rights under these rules;
- practical information on acceptable marketing practices under the opt-in regime including clarification of legitimate collection of personal data;
- practical information for consumers to know how to avoid spam (e.g. use of personal data, etc.);
- practical information for consumers on products and services available to avoid spam (e.g. filtering, security);
- Information on practical steps when confronted with spam, including on complaints mechanisms and ADR systems where available.
- refer to effective industry codes of conduct, complaints mechanisms, labels (e.g. 'trustmarks') and certification schemes where available.
- carry out these awareness activities through different, online and offline, channels, with a view to effectively reaching the various audiences targeted.

In this regard, involvement of industry and consumer associations is important. Co-ordination between the possible various initiatives should be ensured.

IV – Actions by the Commission /Commission services

The Commission will monitor the implementation of the actions summarise above during 2004, including via the informal group on unsolicited communications, and will assess by the end of 2004 at the latest whether additional or corrective action is needed.

As a general rule, the Commission will continue to closely monitor the implementation of the Directive. It will in particular look to confirm that national transposition measures provide for real sanctions in the event of a breach of the relevant requirements, including where appropriate financial or criminal sanctions. (The Commission has launched infringement proceedings in November 2003 against a number of Member States, which have failed to notify their national transposition measures.) The Commission services are willing to assist Member States if needed;

The Commission services have created an informal online group on unsolicited commercial communications, with the support of Member States and data protection authorities. The group will facilitate work on effective enforcement (e.g. complaints, remedies, penalties, international co-operation) and on the other actions identified in this Communication;

The Commission services will ask the Article 29 Data Protection Working Party to adopt an opinion on some concepts used in the Directive on Privacy and Electronic Communications as quickly as possible, in order to contribute to a uniform application of national measures taken under the Directive;

The Commission services have started to investigate, together with Member States and national authorities involved with enforcement, how best to ensure cross-border enforcement inside the EU and with third countries This work with national authorities will continue throughout 2004;

The Commission will support Europe-wide online codes of conduct for direct marketing, and if appropriate their approval the Article 29 Data Protection Working Party;

The Commission will host an OECD workshop on spam in February 2004 and will discuss follow-up actions with Member States, including OECD work to promote effective legislation internationally, awareness, technical solutions, self-regulation, and international co-operation on enforcement;

The Commission will also investigate how best to follow-up the results of the 2003 World Summit on the Information Society in the UE, taking account of the Tunis Summit to be held in 2005;

The Commission has published a call for proposals under the Safer Internet programme where projects could be proposed to deal with spam under various actions; the Commission is currently preparing a proposal for a follow-up programme, Safer Internet *plus*, which will propose funding of further measures to deal inter alia with spam;

The Commission services will continue to provide information on the basics of opt-in on the EUROPA website. It will also provide references via hyperlinks to national implementation aspects, as well as on basic figures and trends on spam where available. The Commission services will also use the Euro Info Centres to disseminate information on the new rules.