



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 24 November 2004

15148/04

TELECOM 174

NOTE

from : The Presidency
to : Delegations
No. Cion prop. : 5691/04 TELECOM 11

Subject : Unsolicited communications for direct marketing purposes or spam
- Presidency Paper

1. INTRODUCTION

Spam is an increasing problem, both in number and in the criminal nature of it. The methods of spammers get more and more sophisticated and due to more and more illegal applications the business case gets increasingly interesting to spammers. Worldwide there is agreement amongst countries that the battle against spam and its malicious practices is to be fought actively. Within the EU, member states also agree on the urgency of this problem.

The Presidency sees spam as a priority issue in the internet security field and stresses the need for short term actions. Since the problem is very complex, multifaceted, and moreover worldwide (no geographical boundaries) and growing rapidly, it is our opinion that the search has to be for short-term practical measures and quick wins without of course losing sight of longer term, lasting solutions. We have no time to waste!

This Presidency Paper expresses our view on the ways to come to concrete results in the battle against spam and the role of the EU and the European Commission. It will be on the agenda of the Telecommunications Council on December 9th 2004, where Ministers may draw some general conclusions on the way forward.

2. DEVELOPMENTS IN 2004

In January 2004 the Commission released a communication on spam¹, identifying a number of actions for all relevant parties (Commission, member states, industry, etc.) in a multilayered approach. In the Telecommunication Council on March 8th 2004 Council Conclusions were adopted. This chapter gives a short summary of what has happened since.

- In most member states the e-Privacy Directive² has been implemented in national law. A review is foreseen 3 years after coming into force, i.e. not later than October 2006.
- The Commission has brought together the different authorities that are responsible for national enforcement (the Data Protection Authorities, the Consumer Protection Authorities and the National Regulatory Authorities). This has led to a very useful contact network of spam enforcing bodies (CNSA). In a joint action the French and Dutch NRA's (CNIL and OPTA) have worked on a cooperation protocol, that as been agreed upon by other countries and will come into force before the end of 2004³.

¹ Document COM(2004)28.

² Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

³ "Cooperation procedure concerning the transmission of complaint information and intelligence relevant to the enforcement of article 13 of the privacy and electronic communication directive".

- In several multilateral fora the work on spam has been put high on the agenda. The OECD has organised two workshops in 2004 (in Brussels in February and in Busan, South Korea in September) and has installed a Task Force working on a toolkit on spam. The ITU has organised a thematic meeting on spam in Geneva in July. Furthermore the problem of spam can be addressed in the preparations for the 2nd World Summit on Information Society (WSIS) in November 2005.
- In October 2004 the Commission and the Dutch Presidency jointly sent out a questionnaire to assess the effectiveness of the actions taken to date and to determine by end 2004 if additional or corrective action is needed. An open workshop on the results of this questionnaire was organised in Brussels on November 15th.

3. CONCLUSIONS

The results from the different activities mentioned above tend to lead more or less in the same direction. Both in broader multilateral fora and in the EU there seems to be agreement on the general action lines. This is also clearly visible in the results of the EU questionnaire: although there are small differences in priorities or specifications, there is a certain similarity in the overall response of the questionnaire. There are some general conclusions to be drawn:

3.1 The need to harmonize the legal framework

Looking at international enforcement cooperation we can conclude that there are a lot of problems to be solved. The implementation of enforcement differs from country to country. The answers on the questionnaire make it more precise: all member countries have implemented the Directive 2002/58/EC, but the variety in implementation is large. Some important differences are:

- administrative or judiciary enforcement, or even a combination
- enforcement by Data Protection Agencies, Consumer Protection Agencies or National (Telecom) Regulatory Authorities.
- variety in financial penalties (from € 145,- per spam message to an administrative fine of € 450.000,-) and other sanctions (warning to offenders, the ability to terminate a business, enforce cessation of spam activities, confiscation or erasure of the offender's data and records to imprisonment)

- opt-in regime for natural persons vs legal persons

These differences, in combination with other legislation like privacy laws, make that it is a necessity and a real challenge to come to a more effective cross-border cooperation.

3.2 The need for improved international cooperation

As has been concluded already many times before, all member states stress the importance of international cooperation. Participation in activities at multilateral level is highly valued by all countries. Important activities here are the OECD Task Force on Spam and the WSIS Working Group on Internet Governance (WGIG).

Also on enforcement there is still a lot of work to do on cooperation. *Within the EU*, according to the answers on the questionnaire, there is a strong demand for boosting intra-EU coordination on information exchange, cross-border complaints and enforcement. The CNSA principal agreement is an important step forward, but there is a need to conquer the problems in exchange of information and cooperation. Concerning the cooperation *outside the EU* a substantial majority of the member states recommends global alliances and a cooperative policy at EU-level with those countries that are the source of the vast majority of (international) incoming spam, like the USA, Far Eastern countries (China, Korea) and Russia.

3.3 Awareness

Another key element is awareness. For a large part, spam is a **security problem**. If all end-users would properly secure their systems, it would be much more difficult for spammers to reach their goals. Therefore, individual end-users are responsible for keeping their systems secured. They must be aware of the consequences -not only for themselves but also for others!- of not using firewalls, antivirus software, spamfilters, etc. and they need to realize the danger of giving private information to unknown people or organizations. But to be aware of this, they need to be well informed. They need to have information on threats and risks, and how to eliminate these. This empowerment of the end-user is an essential part of the fight against spam and we see an important role and ongoing responsibility for governments there.

3.4 Stimulate technological developments

There are already initiatives to come to technical and other measures, such as e-mail identification, authentication and filtering techniques. But we have to consider that spammers will try to circumvent these measures from the moment they are introduced. It is therefore essential that research and development take into account fast developing practices (like phishing) that can't always be foreseen for a long term. There is an important role of the industry here.

4. **RECOMMENDATIONS BY THE PRESIDENCY**

The Presidency attaches great importance to the response to the questionnaire and the outcome of the workshop discussions. In our view there is both the need and the momentum to come to concrete actions now. It is therefore that this paper presents the following presidency recommendations to the Council.

4.1 Harmonisation of the legal framework

We would strongly suggest that the review of the e-Privacy Directive is not postponed to the end of 2006, but will be started shortly in 2005. When we look at the diversity in the national legal frameworks within the EU, it is obvious that although the Directive intended to harmonize the opt-in regime within Europe, in practice the legislation and moreover the enforcement differ a lot and cross-border cooperation is still difficult because of legal and jurisdictional limitations.

However, the problem is increasing on us every day. It is not only the amount of spam, but also the new threats in combination with spam like phishing, identity-theft, etc. that make it necessary to act in short time. We cannot afford to loose time on this! It would therefore be important for the Council to invite the Commission to start up the review as soon as possible.

4.2 Improvement of international cooperation

A very important element is international cooperation, both in developing a common strategy and in enforcement.

Enforcement:

Within the EU the work on cooperation between EU member states has already started, but we still have to improve it. The CNSA principal agreement is a very good initiative for cooperation between enforcement agencies.

Regarding cooperation *outside the EU* there is general agreement on the need for cross border cooperation, especially towards countries from which a large percentage of spam is originating. The Presidency would like to emphasize that in our view a **multilateral approach** is needed. International cooperation should no longer be initiated bilaterally per country, but multilateral, at EU-level. We recommend that the Commission takes an active role in initiating this, of course in close cooperation with the member states.

Strategy Developing:

The WSIS Working Group on Internet Governance offers us a great opportunity to put spam high on the political agenda worldwide. With the help of EU-coordination on the preparation of the WGIG, this is a good chance for the consecutive Presidencies and the Commission to initiate and coordinate a joint EU point of view. As noted in the Coreper guidelines on internet governance it is highly important to have spam high on the agenda of the WGIG.

4.3 Awareness

Several member states have already started awareness activities. However, in the battle against spam awareness on a safer use of internet will be a continuing task for governments. It is important that member states can learn from each other and exchange ideas and experiences on awareness campaigns. Although the actual materials are not exchangeable due to language restrictions, exchanging best practices will be very useful. The (extended) EU Safer Internet programme 2003-2004 has stimulated the forming of national awareness nodes. We advise the Commission to promote coordination and exchange between these national nodes.

4.4 Stimulate technological developments.

In some of the reactions to the questionnaire, some possible solutions were suggested that need to be further explored⁴. Besides that, several private initiatives are being developed by industry. It is important to stimulate and coordinate the development of technical solutions, preferably at EU-level. We would welcome any Commission initiative to invite the industry to come with more solutions.

Furthermore, we think that R&D in the field of combating spam should be increased. Bearing in mind the often expressed wish to increase ICT-related spending within the EU's research programs, we would welcome any Commission initiatives in this respect.

⁴ For example: labelling of direct marketing e-mail, convincing representatives of all actors⁴ to establish a serious study on viability of voluntary and multi-party (self-regulation) approaches to implement "sender pays" mechanisms, efforts against viruses as they are now often used by spammers to convert PCs of broadband users in zombies, identification and authentication mechanisms and better filter techniques.