

April 2004

## ETNO Reflection Document on Unsolicited Commercial Communications (SPAM)

### **Executive Summary:**

ETNO members are fully committed to develop active measures to combat unsolicited commercial communications (spam). Telecom operators are focusing their efforts on awareness raising, technical measures like filtering and the use of various kinds of lists. ETNO believes that public authorities (EC, OECD...) can play an important role in co-ordinating and harmonising the implementation and use of reliable black lists.

ETNO supports all efforts to fight against spam as it is a nuisance not only for users but also for network providers. Building trust and confidence for both providers and consumers is essential for the development of the Information Society and a top priority for telecom operators.

According to conservative estimates, 30-40% of the total amount of e-mail is spam. If this negative trend continues to grow, it will impact the development of new e-mail services and pose a real threat to the success and viability of e-mail as a means of communication.

ETNO members are actively fighting spam through various initiatives - awareness raising, the development of technological solutions, the elaboration of codes of conduct etc. - which require a lot of investment. In such a fast paced industry, such measures, to be efficient, need to be developed through a market driven approach. ETNO members are also considering ways to reduce the appeal of spam, for example, through payment mechanisms for spam-like mail or registration systems that could assist in identifying potential spammers.

Experience shows that adopting legislation is a first necessary step but is only part of the answer. Neither a European opt-in nor opt-out system for unsolicited commercial communications will stop spam, because spam mainly originates from third countries (e.g. United States, Korea, Brazil).

Only a marginal amount of spam has its origin in EU/EEA countries and spammers are unlikely to comply with rules. Despite the new legislation in place in EU (opt-in), operators note that spam is not decreasing, on the contrary the phenomenon of spam is increasing alarmingly. ETNO is in favour of a harmonised approach to achieve a level-playing field for all actors involved across the EU. Industry needs clear rules to avoid competitive disadvantages.

Considering the complexity and variety of aspects linked to fighting spam, it is essential to establish a close dialogue between all players to fully understand what is at stake and find means to fight it efficiently. A dialogue between public and private sectors is key to successfully tackling the challenges resulting from spam. Although spam affects all ICT users (consumers, industry and public administrations) telecom operators as owners of e-communications networks have significant expertise in implementing clear policies and concrete measures to reduce and fight against spam. Therefore, ETNO and its member companies are eager to exchange expertise in the fight against spam with public authorities at the EU and international level.

## How operators try to fight against spam?

ETNO wishes to stress the important actions operators are developing to limit the negative impact of spam on networks and users.

### 1. Awareness raising - empowering users

Operators are undertaking major **awareness campaigns**, informing users of those acts that are prohibited under the current regulatory framework. Reliable information about what spam actually is, advice and practical tips on how to reduce the risk of spam are all important measures.

Furthermore, operators provide customers with clear information on how to report and complain about spam. In order to **manage claims in a diligent manner**, by improving the handling of such claims, operators are simplifying and facilitating the claim process for the user.

In addition, specific provisions in ETNO member companies' terms and conditions prevent customers from using their e-mail accounts for sending spam. Companies have set up "Abuse Departments" with efficient follow-up routines regarding complaints related to spam-abuse of their networks. This approach is being further developed through co-operation with other telecommunication companies both nationally and internationally. To this effect some companies have initiated a European Abuse Forum to ensure greater involvement of all industry stakeholders.

ETNO members' experience shows that spam originating from their own customers and distributed via their own networks is a very limited problem, mainly thanks to the fact that there is a clear policy on spam and well-functioning abuse departments that closely follow-up on claims of abuse.

### **Using black lists and white lists**

**Black lists:** consist of lists of unaccepted senders. These are implemented through the entry servers to filter which servers may send us e-mail, in other words, from which servers e-mail is accepted. There are various types of black lists.

**Anarchist black lists.** Unfortunately, the majority of black list projects are being managed by anarchists or anti-spammers who do not understand the magnitude of the problem, and who believe that its eradication is a game. These initiatives, not always very serious, are hindering operators and having no contact address, their initiators evade all responsibility.

**Commercial black lists.** These are managed by companies involved in finding solutions to fighting spam, collecting junk mail messages that circulate over the Internet, analysing their origin and adding these IP addresses to their lists. They can be trusted and have mechanisms so that operators may eliminate traffic from selected IP addresses, once the problem has been resolved. Operators are closely monitoring the effectiveness of these lists although there currently are only a limited number of commercial lists. It should be noted that in some countries, black lists raise data protection concerns and entail consent requirements.

**White lists:** consist of generating a list of accepted senders (servers as well as e-mail addresses or domains). However, these lists are restrictive and not very functional.

**Robinson lists:** the famous Robinson lists have been a failure. The initial idea of recording in a list of addresses which did not want to receive commercial e-mail and which marketing companies had to consult and comply with, has turned against itself. These lists have been consulted by unscrupulous and malicious spammers and have been repeatedly sabotaged.

## **2. Using technical solutions**

Furthermore, industry is investing in the development of costly anti-spam filtering and other technical solutions. It is important to continuously improve and adapt industry's response to spammers, as they keep on developing new tactics to attack information systems and networks and circumvent technical solutions.

Public authorities should not jeopardise or hinder the development of new technical solutions through inappropriate regulation or by imposing specific technologies to fight against spam. Industry should be free to develop new solutions through a market driven approach without regulatory or policy barriers. For example, existing anti-spam filters for incoming emails can not in some cases be activated as a default option due to data protection legislation restrictions (the consent of the customer)

**Filters for incoming mail:** 90% of anti-spam commercial solutions focus on blocking the entry of the undesired e-mail. They are offered as an additional service to mail solutions. By using these filters, it prevents the user from seeing his mailbox inundated with spam. It can consist of:

- A filter using "signatures" and black lists.
- A filter using heuristic and Bayesian techniques - i.e. focusing on the identification of mails and on filtering technology based on predefined words. Currently tests are being conducted on various solutions.

**Filter for outgoing mail:** studies are being conducted on the technical, legal and economic feasibility of this kind of filter. Some operators are about to implement very costly systems for blocking outgoing mail. This way, all outgoing mail from ISPs customers are sent via the ISPs own mail platform which facilitates control and scanning. Controlling outgoing mail is likely to be very efficient in the fight against spam.

Telecom operators offer filters as a commercial service (Golden Service) or as a free service. Very often they use a combination of different solutions to minimise the spam problem, for their own operations (network, abuse and support costs), users and for other ISPs and customers of these ISPs.

In order to effectively fight spam and the creativity of spammers, not only advanced technological solutions are needed, but automatic updating of the filters must be offered to consumers and businesses alike.

## **How public administrations can contribute to fight against spam?**

In addition to the actions carried out by industry, mobilisation of the regulatory authorities (at the national level, the Community level and at the international level) is essential in combating this global problem. ETNO therefore welcomes the EU's decision to actively confront the issue.

As stated by Commissioner Liikanen on various occasions, spam is a global problem, hence the **importance of international co-operation** in this respect (different jurisdictions and legislation). Given that the majority of unsolicited commercial mails originate from outside the European Union, international co-operation is key to combating the problem.

ETNO considers it a top priority for the European Commission to develop an active policy of multilateral as well as bilateral agreements with third countries, more specifically with the United States and other countries where spam mainly originates from (Korea, Brazil).

Regulatory authorities should not lose sight of the need to develop information, education and **end user awareness campaigns**. Recognising the important role that the industry can and must play, public authorities should also take their share of responsibility in **promoting proper use of the Internet amongst citizens** (for example, through awareness and information advertising campaigns). This would complement efforts carried out by industry to empower users in fighting spam, making it less effective and preventing large quantities of spam from being generated by vulnerable computers.

It is equally important that Internet users are aware of their rights under the new soft opt-in regime set by Directive 2002/58/EC in order to avoid confusion when legitimate solicited commercial messages are sent out. ETNO wishes therefore to stress the importance of distributing balanced and accurate information to European consumers and businesses on the new Data Protection Directive (cf Danish Consumer Ombudsman's web pages on e-commerce <http://www.net-tjek.dk/>).

The European Commission and the national authorities could also be involved in developing a type of "**official black list**"; the fact that it was officially supported would give them a seal of guarantee with users and the industry. The Commission could also promote the **handling of claims by the Administration**, for example, through the National Data Protection Agencies).

## Conclusion

ETNO members wish to reiterate their full commitment to developing active measures, including cooperation, to combat the massive sending of unsolicited commercial communications.

As the European Commission has expressed, spam must be fought on several fronts (legal, technical, global and through awareness raising). Spam will not be effectively tackled without a joint effort of all actors involved combining all legal and technical measures at global level.

ETNO member companies are focusing their efforts to fight spam on the following points:

- **Awareness raising.** Good information to customers and advice on how to handle spam.
- **Technical measures.** Offering effective and secure filters to stop viruses and spam as well as blocking pc's and servers that distribute

spam using their networks. ETNO members are committed to innovate further and pursue new technological solutions against spammers. However, these efforts are not the unique solution; they are only part of a global answer.

- **Lists.** ETNO believes that Public authorities (EC, OECD...) can play an important role in co-ordinating and harmonising the implementation and use of reliable Black Lists. Official third party approval of these lists would provide users and industry with a seal of guarantee. ETNO as a major voice of the ICT industry is looking forward to provide its expertise and experience to explore the possibility of setting-up an "official" list (with transparent procedures, appeal mechanisms and functioning).