June 2006

ETNO Reflection Document as an input to a future European Commission Communication on SPAM

Executive Summary
ETNO members are fully committed to develop active measures to combat unsolicited commercial communications (spam). ISPs and network operators have an important role in the fight against spam. Therefore they are focusing their efforts on awareness raising, technical measures like filtering and the use of various kinds of lists. As there is not a single solution to combat spam, ETNO believes that a consistent and co-ordinated approach by all stakeholders involved (private and public) at the international level is needed.

PRELIMINARY CONSIDERATIONS

ETNO is grateful for the opportunity it has been given by the European Commission to express its views on the future Communication on spam, spyware and malware.

ETNO members are fully committed to developing active measures to fight abuses involving Internet services. ETNO members are putting all their efforts into maximizing information and network security, and optimising the handling process for all types of abuse.

Therefore, ETNO supports any action designed to increase trust and confidence in Internet services. For instance, spam is a phenomenon not only affecting Internet users, but also electronic communications network operators and Internet service providers (designated as "operators" henceforth). While most end-users see the problem of spam mainly as the fact of receiving undesired e-mail, operators must also deal with spam traffic exchanged at network level, and spam generated from their own networks, with the resulting impact on the dimensioning of the network as well as the quality of service.

The world of IP communications is changing, so is spam: it is clear that some spam is now being made via SMS service on fixed and mobile networks and that "traditional" spam is moving to SPIT (Internet Telephony spam). SPIT, like its close relatives spam and SPIM (instant messaging spam), takes advantage of technology's ability to quickly automate routine tasks at a negligible cost. For telemarketers, SPIT is much cheaper than employing a call centre staffed with live human operators. For the recipient, SPIT is much more costly than spam in terms of time and annoyance.

SPAM, SPIM and SPIT are cross-border issues, therefore a legislative framework forbidding unsolicited commercial communications like in Europe is only one element in managing the spam phenomenon as a whole, but it is even more important that this regulatory framework encourages cooperation between various competent national authorities.

Based on a clear commitment towards customers and society as a whole, ETNO would like to share its comments and experience with the European Commission and ETNO sincerely hopes that these remarks will help the EC when preparing future actions. These actions are necessary at the highest level and in a co-ordinated manner to combat this reality of spam, which is jeopardising the success of the Internet.

MEASURES DEVELOPED BY ETNO MEMBERS TO FIGHT AGAINST SPAM

Spam began as annoying unsolicited commercial communications, but in the meantime spam has not only grown exponentially but it has evolved into dangerous messages often used as a vehicle for spreading viruses, phishing, and more generally scams of a growing nefariousness and diversity. Indeed, spam has turned into a security issue for customers: viruses, worms are disseminated on a high percentage by spam generated by PC zombies.

ETNO wishes to stress the important actions operators are developing to limit the negative impact of spam and other on-line threats on users and networks:

1. **Protect the email service infrastructure and the end-user equipment from external abuse**

2. **Identify and counteract abuses inside an operator's network**

3. **Handle claims for abuses lodged by customers or third parties**

4. **Co-operate with other players in the information society**

5. **Develop and implement secure products, services and networks**

6. **Inform and educate customers about Internet security**

1. Protect the email service infrastructure and the end-user equipment from external abuse

During the 4th quarter of 2005, the amount of spam in the total amount of email traffic coming into an ISP's network was 80%[1]. This means that up to 4 out of 5 inbound emails must receive some kind of treatment by the receiving operator. This treatment can include operations like cleaning the email from a known virus, or tagging the email when automatically recognised as spam, etc.

ETNO members have deployed measures to keep this flood of abusive emails from harming both their email service infrastructure and the end-user equipment, and are doing so in conformance with existing legislation.

In order not only to safeguard, but improve this ability to eliminate most, if not all, spam at the entry gate, ETNO members encourage awareness raising among stakeholders of the private and public sector, relating to the extent and nature of the spam phenomenon. Only then can a proper balance be met between privacy and security needs.

2. Identify and counteract abuses inside an operator's network

It is mainly through the constant supervision by an operator of its email service infrastructure (in addition to other measures at the technical level and at the generic level, such as customer awareness, handling of claims…) that the risk of abuse can be decreased.

ETNO members monitor the use of their email resources and limit their access to legitimate users. While conforming to existing legislation, some operators also attempt to identify those end-users terminal equipments infected with spam relaying viruses, a well known source of the majority of spam circulating worldwide (a

[1] Traffic measured in response to a sollicitation from the OECD, from 1/10/05 to 31/12/05 on 127 million mailboxes from ISPs in several countries including the USA; see http://www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf

consequence of the "zombie problem"). Identification can be carried out with the help of claims for abuses sent by other operators who are receiving the spam (see also next section). In most cases, the end-user is not aware of the situation and a warning letter sent by the operator with virus-cleaning and PC-repair instructions is a way to solve the problem.

3. Handle claims for abuses lodged by customers or third parties

The handling of incidents or abuses related to Internet services in an efficient manner is critical.

ETNO members have established efficient procedures to deal with abuse claims that originate from their customers or from other networks and concern their customers or networks.

In order to deal efficiently with claims, ETNO members do:

- Designate specific groups to handle incidents and/or abuses.
- Publish the channels for entry to these abuse handling groups in each company
- Handle claims in accordance with common and uniform processes

ETNO members have specific groups to deal with claims and publish their channels for handling Internet abuse, the mailboxes for abuses or other channels via which customers or any Internet user can lodge claims for abuses, where this information is constantly updated. The most common mechanism is based on standardised mailboxes (RFC2142), such as abuse@operator.com and postmaster@operator.com which are generally used around the world to deal with this type of incidents.

The groups in charge of handling claims establish processes involving actions to be taken regarding any abuse committed, based on the type of abuse, the number of incidents involved over time, the urgency or importance of the abuse, etc. These processes are designed to put an end to the abuse reported, as well as to inform customers about the problem that occurred with their terminal equipment.

4. Co-operate with other public, private players in the information society

Since many players (public, private) are working simultaneously to try to reduce any kind of Internet abuse, greater co-ordination is desirable at all levels:

- industry co-operation with the competent enforcement authorities (such as national DPAs, national Consumer Protection Agencies, etc.)
- industry co-operation with international organisations and participation in supranational debates

Indeed, industry and competent enforcement authorities need to strengthen co-operation in the enforcement of anti-spam legislation, by sharing generic information on spam abuses that occur on the networks.

At the national level, in some countries independent foundations are in place combating spam by running abuse desks, maintaining blacklists, etc. In such cases involvement of ETNO members can vary from sponsorship to even founding membership.

At the international level, ETNO members are participating in those initiatives that can come up with some solutions to the spam problem and co-operate with the public sector, as in the OECD's Anti-Spam Task Force, through BIAC. This enables using legislation for an optimal effectiveness of the technical measures against abuse, and results in constantly improving industry best practices.

ETNO particularly welcomes the OECD Anti-Spam Toolkit[2], recently finalised by the OECD Anti-Spam Task Force. This is a global initiative addressing what is a global problem, and gives useful indications on all fronts of the battle (regulatory, enforcement, education, technology, etc).

The Toolkit includes in Annex 2 a list of high-level **best practices for operators, set by the industry**[3]. ETNO members regard this document as a major global reference for the deployment of technical solutions, but also insist that it must really be a living document, in view of the pace of technology change, and are ready to contribute.

The fact that technical solutions are, in their principle, the same everywhere in the world, is also a strong argument for a common approach internationally among law makers and regulatory authorities. ETNO and its members, in their proper role, will actively contribute to the post-WSIS Internet Governance Forum - the multi-stakeholder policy dialogue with spam in its remit. Operators expect that industry will be widely consulted on the policy options presented or supported by the European Commission in the IGF.

In addition to that the EU should advocate in international fora that third countries that are major exporters of spam do also implement

[2] The OECD Anti-Spam Toolkit is downloadable from http://www.oecd-antispam.org/
[3] The BIAC-MAAWG best practices for ISPs and network operators, see http://www.oecd-antispam.org/article.php3?id_article=232

adequate regulatory and enforcement measures in order to solve or reduce this global problem.

5. Develop and implement secure products, services and networks

The security of services offered by ETNO members begins with the design and development phase of such products and services, as well as with their implementation in the network systems and technologies.

In the development phase of future products and services, ETNO members are developing detailed studies on potential weaknesses of a given product or service with regard to their security for customers as well as the risk of abuse or misuse by third parties. This is essential to guarantee that those products and services will be secure.

In the event a customer's equipment has a security problem, which results in some type of abuse, ETNO members provide and make available to customers, through appropriate commercial policies, tools that complement the security of use of the services provided, allowing them to protect themselves against any abuses that might occur.

In developing their network systems and technologies, ETNO members are also evaluating opportunities and implementing technologies that will minimize the negative consequences on network performance and customer services in relationship to abuse such as spam and malware.

6. Inform and educate customers about Internet security

ETNO members are one of the driving forces behind the Information Society and are fully committed to campaigns designed to inform and "educate" customers about security.

ETNO members have not lost sight of the need for a policy of information, education and **awareness to end-users** (via helpdesks, web pages). If Internet users were really aware and knew how to properly act, they would naturally implement secure habits in the use of Internet, and receive (or emit) less spam (and viruses). Thus ISPs could prevent large quantities of spam from being generated by vulnerable computers.

Therefore also with technical support ETNO members encourage their customers to protect their computers with up-to-date anti-virus software, protect their mailboxes with up-to-date anti-spam software, and protect their identity on-line at least as well as they do off-line.

ETNO recognises the important role that the industry as a whole must play in this policy of information to and awareness of its customers. However Public Authorities should also take their share of responsibility in promoting proper use of the Internet amongst its citizens (for example, through awareness and information advertising campaigns).

CONCLUSIONS

Considering the global dimension of spam and more recent phenomena such as spim or spit, experience has shown that the current EU regulatory framework for unsolicited commercial communications has had little effect in reducing spam. It must be accompanied by strong technological solutions, deployed by industry in a legislative environment that is free of uncertainties and internationally coherent.

ETNO members think it is essential to maintain a close dialogue between all stakeholders to fully understand the threats and agree on the responses efficiently.

Therefore, it is essential that the dialogue also exist at a global level. The OECD Anti-Spam Toolkit and its annex on ISP best practices therefore constitute an obligatory reference for ETNO members.

As spam is also a security threat (dissemination of spyware, phishing, identity theft...), cooperation between public and private sectors needs to continue and should be aimed at the promotion of secure and reliable e-communication services for all.