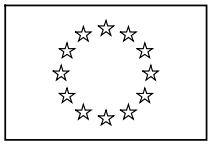

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 22.01.2004
COM(2004) 28 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on unsolicited commercial communications or 'spam'

TABLE OF CONTENTS

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on unsolicited commercial communications or 'spam'

(Text with EEA relevance)

EXECUTIVE SUMMARY

Unsolicited commercial communications by e-mail, otherwise known as 'spam' have reached worrying proportions. More than 50 percent of global e-mail traffic is now estimated to be spam. What is even more worrying is the rate of growth: in 2001 the figure was 'only' 7 percent.

Spam is a problem for many reasons: privacy, deception of consumers, protection of minors and human dignity, extra costs for businesses, lost productivity. More generally, it undermines consumer confidence, which is a prerequisite for the success of e-commerce, e-services and, indeed, for the Information Society.

The EU anticipated this danger, and adopted in July 2002 Directive 2002/58/EC on Privacy and Electronic Communications, that introduced throughout the EU the principle of consent-based marketing (opt-in) for electronic mail (including mobile SMS or MMS messages), and complementary safeguards for consumers. The deadline for implementing the Directive on Privacy and Electronic Communication was the 31st of October 2003. Infringement proceedings have been opened against a number of Member States that failed to notify transposition measures to the Commission.

While adopting legislation is a first, necessary step, legislation is only part of the answer. This Communication identifies a series of actions that are needed to complement the EU rules and thereby make the 'ban on spam' a reality.

There is however no 'silver bullet' for addressing spam. The series of actions identified in the present Communication focus in particular on effective enforcement by Member States and public authorities, technical and self-regulatory solutions by industry, and consumer awareness. The international dimension is also singled out, since much spam comes from outside the European Union.

While these actions broadly reflect the consensus that emerged in the course of 2003, as confirmed at a public workshop held in October 2003, consensus on their implementation will also be of essence. Only if everyone, from Member States and public authorities, through businesses, to consumers and users of the Internet and electronic communications play their role will the proliferation of spam be curtailed.

Some of these actions have an obvious cost. But this is the price to pay if e-mail and e-services are to survive as an efficient communication tool. Implementation of the actions

identified in this Communication will go a long way toward reducing the amount of spam, for the benefit of the information society, our citizens and our economies.

Background and Purpose

Unsolicited commercial communications by electronic mail[1], otherwise know as 'spam', are widely recognised as one of the most significant issues facing the Internet today. 'Spam' has reached worrying proportions. At present, there is a risk that users of e-mails or SMS simply stop using e-mail - one of the favourite Internet applications - or mobile services, or refrain from using it to the extent that they otherwise would. More generally, since the Internet and other electronic communications (e.g., broadband access, wireless access, mobile communications) are expected to be a key element for the growth of productivity in modern economies, 'spam' requires even closer attention.

While there is a consensus that action is needed before the benefits brought to businesses and citizens by e-mail and other e-services are offset by the proliferation of spam, how best to combat spam is not self-evident. More importantly, there is no 'silver bullet' in this fight. Only if everyone, from Member States and competent authorities, through businesses, to consumers and users of the Internet and electronic communications plays their role will there be a chance to tackle spam efficiently.

The present Communication identifies actions on the various legal, technical and awareness fronts, building on Directive 2002/58/EC, establishing an 'opt-in' (consent-based) regime which Member States had to implement for commercial communications by the 31st of October 2003[2].

This series of actions focus in particular on the effective implementation and enforcement of this Directive by Member States, technical measures, industry self-regulation, consumer awareness, and international co-operation. The international dimension is indeed crucial, since much spam seems to come from outside the European Union, and in particular from North America[3].

These actions broadly reflect the consensus that emerged in the course of 2003, as confirmed at a public workshop held in October 2003[4]. Consensus in this area is all the more important since it is primarily for those interested parties, with the support of the

---

1 The present Communication does not cover unsolicited communications offline, e.g. unsolicited (postal) mail.

2 See in particular Article 13 of Directive 2002/58/EC on Privacy and Electronic Communications and Privacy (see section 2, below).

3 For instance, the 'spam box' initiatives organised in 2002 by respectively the French 'Commission Nationale Informatique et Libertés (CNIL)' and the Belgian 'Commission de la Protection de la Vie Privée (CPVP)' seemed to confirm that the United States and, to lesser extent Canada, were the primary source of spam messages. The CPVP findings are available at: http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf; the CNIL report is available at the following URL address: http://www.cnil.fr/thematic/docs/internet/boite_a_spam.pdf. See also: UNCTAD, E-Commerce and Development Report 2003, New York and Geneva, 2003, p. 27.

4 An issue paper 'on unsolicited communications or spam' was distributed in advance of the workshop on the subject. The issue paper itself built on previous discussions in the context of the Communications Committee (COCOM) and with the Article 29 Data Protection Working Party. In response to a questionnaire, information was provided by members of the COCOM and of the Article 29 Data Protection Working Party. A number of industry associations or individual companies also reacted, from ISPs and communications operators (mobile and fixed) through direct marketeers and advertisers, to computer and software manufacturers.

Commission where possible, to implement the actions identified, for the benefit of the information society, its industry and its users.

Structure of the document

The document identifies specific aspects of the spam 'problem', and proposes specific actions to be taken to address each aspect in turn. Best practices have also been singled out whenever useful.

Proposed actions are presented according to the following structure:

- **Implementation and enforcement actions** for governments and public authorities in particular, in areas like remedies and penalties, complaints mechanisms, cross border complaints, co-operation with third countries, monitoring (Section 3).
- **Self-regulatory and technical actions** for market players in particular, in areas like contractual arrangements, codes of conduct, acceptable marketing practices, labels, alternative dispute resolutions mechanisms, technical solutions e.g. filtering, security (Section 4).
- **Awareness actions** covering prevention, consumer education, reporting mechanisms, to be taken by governments and public authorities, market players, consumer associations and the like (Section 5).

A table at the end of this Communication provides a summary of these actions. These actions are related to each other in several ways. As much as possible they should be implemented in parallel and in an integrated fashion.

Before turning to these actions, the next sections briefly analyse 'spam' as such (section 1) and recall the new rules applicable since the 31st of October 2003 (section 2).

1. SPAM – THE PROBLEM

Spam': What is it?

'Spam' is a term more often used than defined. In short, it is commonly used to describe unsolicited, often bulk e-mails. The new Directive does not define or use the term 'spam'. It uses the concepts of 'unsolicited communications' by 'electronic mail', 'for the purposes of direct marketing' which taken together, will in effect cover most sorts of 'spam'. Therefore, the concept of 'spam' is used in this Communication as a shortcut for unsolicited commercial electronic mail.

Note that the concept of 'electronic mail' itself is intended to cover not only traditional SMTP-based 'e-mail' but also SMS, MMS and, indeed, any form of electronic communication for which the simultaneous participation of the sender and the recipient is not required (see Section 2, below)

1.1. The size of the problem

Unsolicited commercial e-mail, or spam, has reached worrying numbers. Despite variations in statistics, it is generally estimated that more than 50 percent of global e-mail traffic is 'spam'.

The rate of growth is even more worrying. In 2001, spam was estimated to be 'only' 7 % of global e-mail traffic. It was estimated at 29 % in 2002. And the projections for 2003 show an estimated 51 % to be spam.

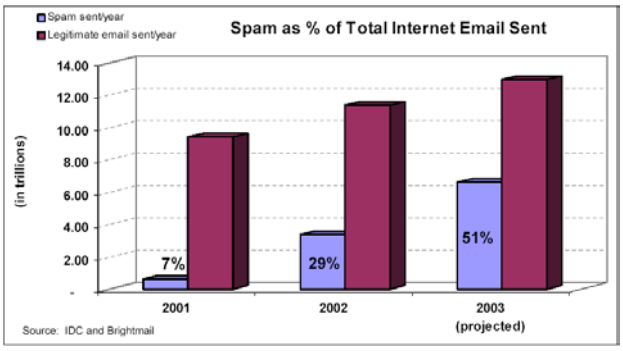

Figure No 1: spam as total internet e-mail sent

There may be considerable variations between categories of users and between regions in the world. (At the European Commission for instance, an estimated 30% of e-mails coming from outside is estimated to be spam.) In general however, recent EU figures are no less worrying than global figures[5].

While unsolicited communication or spam over mobile networks, via e.g. Short Message Service (SMS) text messaging, currently appears to be less of a problem, developments like e-mail over mobile can be expected to increase the volume of spam. Experience in countries with wide I-mode mobile usage (e.g. Japan) confirm this threat.

[5] An estimated 49 % spam in the EU for September 2003, compared to some 54 % worldwide for the same period (Source : Brightmail, 2003).

1.2. Why spam is a problem

From the viewpoint of individuals, spam is an invasion of privacy. This concern is at the heart of the new rules on unsolicited communications described in the next section. Furthermore, spam is often misleading or deceptive. An important proportion of spam appears to be driven by a desire to rip-off consumers through misleading or deceptive statements[6]. Unfortunately all too many consumers do respond to these misleading or deceptive spam[7]. Pornographic messages can also be very upsetting[8]. Cleaning up mailboxes to remove spam is time-consuming for the user, and increases users' costs when filtering and other software facilities are needed.

Do people care?

The number of complaints is one indication of the concerns expressed by users. In 3 months, the French Spam Box had attracted 325.000 messages. A similar experience in Belgium led to 50.000 complaints in 2.5 months[1]. The permanent spam box run by the FTC, called the UCE Database, was attracting 130,000 messages per day in early 2003[1].

Spam has reached a point where it also creates considerable cost for businesses. In terms of direct costs, employees also have to clean up inboxes, thereby undermining efficiency/productivity at work. IT departments spend time and money trying to address the problem. Internet Service Providers (ISPs) and e-mail service providers (ESPs) have to buy more bandwidth and more storage capacity for e-mails that are unwanted. There is also a risk that spam prompts liability for the entity receiving it (e.g., harmful content on employee's PCs) or simply - and unwittingly - relaying it (e.g., wrong blacklisting, damage to reputation). There are also indirect costs: some legitimate commercial or business emails are not delivered due to current anti-spam filtering techniques (so-called 'false positives'), or simply not read anymore due to their association with spam. Spam is increasingly used as a vehicle for spreading viruses, which can prove very costly to businesses.

---

6 According to a recent report form the FTC, 22% of spam analysed contained false information in the subject line; 42% contained misleading subject lines that misrepresented that the sender had a business or personal relationship with the recipient; 44% of spam contained false information in the from or subject lines; over half of finance related spam contained false from or subject lines; 40% of all spam contained signs of falsity in the message; 90% of investment and business opportunities contained likely false claims; 66% of spam contained false from lines, subject lines or message text. (False Claims in Spam, A report by the FTC's Division of Marketing Practices, 30 April 2003, available at: http://www.ftc.gov/reports/spam/030429spamreport.pdf)

7 According to Pew Internet, 7% of email users report they have ordered after unsolicited email and 33% of email users have clicked on a link in unsolicited email to get more information. Even if the percentages of consumers who are ripped off remain relatively low, the phenomenal economies of scale that can be achieved by rogue traders using misleading or deceptive spam have taken the problem of consumer scams to a new level. See: 'Spam–How It Is Hurting Email and Degrading Life on the Internet, October 2003', Report by Deborah Fallows for the Pew Internet & American Life Project. This report is available at the following URL address: http://www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf. A bulk emailer recently testified at the FTC Spam Forum organised in April-May 2003 that he could profit even if his response rate was less than 0.0001%. (Remarks by Timothy J. Muris Chairman, Federal Trade Commission, Aspen Summit, Cyberspace and the American Dream, The Progress and Freedom Foundation, August 19, 2003 Aspen, Colorado).

8 Spam messages sometimes also include gratuitous violence or incitement to hatred on grounds of race, sex, religion or nationality.

Measuring the cost of spam remains a difficult exercise, in particular for individuals, not least because it is difficult to attach a monetary value to some of the harm caused. Estimates are however generally disquieting. As an illustration, Ferris Research has estimated that, in 2002, spam cost European companies 2.5 billion € just in terms of lost productivity[9]. And, as indicated above, the amount of spam has increased considerably since 2002. Software provider MessageLabs Ltd estimated in June 2003 the cost of spam to UK business at about 3.2 billion £[10]. Spam may also have different implications depending on the industries concerned. For instance, the legal sector may be particularly impacted by spam in view of the confidential and sensitive information that it handles.

One of the most worrying consequences of spam is that it undermines user confidence, which is a prerequisite for successful e-commerce and the information society as a whole. The perception that a retail medium is affected by rogue traders can have a profound effect on the reputation of legitimate traders in the same sector. Recent figures in the US, whose experience with spam is more extensive than the EU, confirm that many people are trusting e-mail less because they are receiving so much spam[11].

More generally, the Internet and other electronic communications - broadband access, wireless access - are expected to be a key element for the growth of productivity in modern economies. However, some attractive features of such services – being 'always on', wireless access – are features that can considerably increase the amount of spam received or relayed, if no proper security measures are in place. Perversely therefore, the growth of such services could lead to an increase in spam unless effective measures are implemented rapidly.

2. THE RULES ON UNSOLICITED COMMERCIAL COMMUNICATIONS IN SHORT

2.1. The opt-in regime

The Directive 2002/58/EC on Privacy and Electronic Communications (date of transposition 31 October 2003) requires Member States to prohibit the sending of unsolicited commercial e-mail or other electronic messaging systems such as SMS and Multimedia Messaging Service (MMS) unless the prior consent of the subscriber to such electronic communications services has been obtained (Article 13(1) of the Directive) [12]. This is the 'opt-in' system, which was until now only applicable to faxes and automated calling machines[13].

---

9 Source: Ferris Research, 2003.

10 This figure and other estimates are mentioned in: '"Spam"; Report of an Inquiry by the All Party Internet Group', London, October 2003, p. 8; This report can be consulted via the following URL address: http://www.apig.org.uk

11 According to the recent survey by Pew Internet mentioned above, 25 percent of interviewees were using e-mail less because they were receiving so much spam.

12 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002.

13 For voice telephony marketing calls, other than by automated machines, Member States may choose between an opt-in or an opt-out approach.

Three basic rules under the new regime:

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

Not all unsolicited e-mails are prohibited however. There is an exception to this rule in cases where contact details for sending e-mail or SMS messages have been obtained in the context of a sale. This is sometimes referred to as 'soft opt-in'. Within such an existing customer relationship the company who obtained the data from its customers may use them for the marketing of similar products or services to those it has already sold to the customer. This exception has been harmonised at Community level, and Member States have no choice but to implement it. However, this exception must be strictly drawn in order to avoid effectively undermining the opt-in regime. Nevertheless, even then the company has to make clear from the first time of collecting the data that they may be used for direct marketing (and if appropriate, that it may be passed on to third parties for that purpose), and should offer the right for the customer to object 'free of charge and in an easy manner'. Moreover, each subsequent marketing message should include an easy way for the customer free of charge and easily to stop further messages (opt-out).

The opt-in system is mandatory for any e-mail, SMS addressed to individuals (natural persons) for direct marketing. Member States can extend the opt-in system to communications to businesses (legal persons). Member States that had chosen for an opt-out system for business-to-business marketing, including opt-out lists, can continue to do so. Applying a differentiated regime according to the nature of the subscriber to an e-mail service may lead to specific difficulties for senders when it comes to differentiating legal persons from natural persons.

For all categories of addressees, both legal and natural persons, the Directive prohibits direct marketing messages, which conceal or disguise the identity of the sender. Moreover, those messages must include a valid address to which recipients can send a request to stop such messages[14].

The 'Article 29 Data Protection Working Party', which was set up to advise the Commission and brings together data protection authorities in the EU, is examining some of these concepts more closely in order to contribute to a uniform application of national measures under Directive 2002/58/EC[15]. Consensus on these issues will avoid differences in interpretation that would damage the functioning of the internal market.

---

[14] Article 13(4) of Directive 2002/58/EC.

[15] In accordance with Article 15(3) of Directive 2002/58/EC in conjunction with Article 30 of Directive 95/46/EC.

Other aspects of unsolicited communications have been addressed in previous documents of the Working Party[16].

2.2. Enforcement provisions

The provisions of the 'general' Data Protection Directive on judicial remedies, liability and sanctions are applicable to the provisions of the Directive on Privacy and Electronic Communication, including the provisions on unsolicited communications[17].

In short, Member States must ensure that penalties and remedies are in place for infringements. An individual right to a judicial remedy must be provided for any breach of the rights provided under national law. While this judicial remedy is without prejudice to any (possibly prior) administrative procedures, there is no harmonised requirement to provide for such administrative procedures. There must be an individual right to a compensation for any damage suffered as a result of any unlawful processing or act. There must be sanctions to be imposed in case of infringements, which ensure full implementation of the Directive.

In other words, while the very nature of a Directive means that Member States have a margin of manoeuvre for choosing the measures – including the remedies and penalties - that they take when implementing that Directive, such measures are required to ensure 'full implementation' of the provisions on unsolicited commercial communications.

As is generally the case for a Directive, enforcement of the provisions lies with Member States in the first place, not with the Commission. For instance it is not for the Commission to prosecute, or impose fines on, those who infringe the rights and obligations provided in the Directive[18].

---

16 See for instance Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000; Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union. See also the Harvesting has been discussed in the Working document of 21 November 2000 entitled "Privacy on the Internet"-An integrated EU Approach to On-line Data Protection". These documents can be consulted at the following URL address: http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm

17 Article 15 of Directive 2002/58/EC refers to Chapter III of Directive 95/46/EC on Judicial remedies, liability and sanctions:
Article 22 – Remedies
Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.
Article 23 – Liability
1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.
2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.
Article 24 – Sanctions
The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

18 This differs for instance from agencies like the US Federal Trade Commission.

2.3. Other provisions applicable to 'spam'

A practice often related to 'spamming' is e-mail harvesting, that is, the automatic collection of personal data on public Internet-related places, e.g., the web, chatrooms, etc. Such practice is unlawful, by virtue of the 'general' Data Protection Directive 95/46/EC, whether or not collection is performed automatically by software[19].

Fraudulent and deceptive spam can be particularly offensive. These practices are already illegal under existing EU rules on misleading advertising, unfair commercial practices, (e.g., Directive 84/450/EEC on misleading advertising)[20]. National laws will also generally provide for stiffer penalties in more serious cases, including criminal sanctions.

Specific categories of spam can be even more upsetting, such as pornographic spam or spam including gratuitous violence, in particular when children are exposed to it[21]. While the content of some such messages may be harmful, but not illegal per se, their indiscriminate distribution to adults and children alike will generally be illegal under national law sometimes with quite severe penalties. Spam messages could also contain illegal content, such as incitement to hatred on grounds of race, sex, religion or nationality. In any event, as soon as such messages have a direct marketing purpose - and this will often be the case - they will be caught by the 'ban on spam' like other categories of unsolicited e-mails.

Reference should also be made to the requirement in Directive 2000/31/EC on certain aspects legal aspects of information society services, in particular electronic commerce (Directive on electronic commerce) that 'commercial communications' be clearly identifiable as such (see Article 6 (a) of the Directive on electronic commerce)[22].

Also, activities such as hacking or identity theft are often perpetrated in support of spam activities, in order to send spam or gain access to databases of addresses or to computers.

---

19 See also the Working document of the Article 29 Data Protection Working Party entitled "Privacy on the Internet" - An integrated EU Approach to On-line Data Protection" (Document No WP 37, adopted on 21 November 2000).

20 Council Directive 84/450/EEC of 10 September 1984 relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising OJ L 250, 19.9.1984, p. 17-20. The Commission has recently made a proposal to replace and update the misleading advertising Directive (COM(2003) 356 final).

21 On 24 September 1998, the Council adopted the Recommendation on the development of the competitiveness of the European audio-visual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity (98/560/EC). The Recommendation was the first legal instrument at EU-level concerning the content of audio-visual and information services covering all forms of deliveries, from broadcasting to the Internet.

22 Directive of the European Parliament and of the Council of 8 June 2000, OJ L 178, 17.7.2000. As a general rule, 'commercial communications' must comply with the rules applicable to them in the Member State of establishment of the service provider. This rules does however not apply to the permissibility of unsolicited communications by electronic mail (see Articles 3 of the Directive on Electronic Commerce and its Annex). In the (limited) cases where natural persons would not be protected by Directive 2002/58/EC (e.g. natural persons who are not subscribers) against [0]unsolicited commercial communications, Member States must also ensure under the Directive on Electronic Commerce that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves (see Article 7 of the Directive on electronic commerce).

Many such activities will be covered by the Framework Decision on attacks against information systems, which provides for criminal penalties. This Framework Decision, based on a Proposal of the Commission, has been agreed politically in February 2003 and should be soon officially adopted[23]. Many Member States can already prosecute illegal access to servers or personal computers or their abuse as a criminal offence.

3. EFFECTIVE IMPLEMENTATION AND ENFORCEMENT BY MEMBER STATES AND PUBLIC AUTHORITIES

This section on effective implementation and enforcement covers proposed actions targeted at governments and public authorities in particular, in areas like remedies and penalties, complaints mechanisms, cross border complaints, co-operation with third countries and monitoring.

Before turning to the discussion on enforcement however, the Commission notes that a number of Member States have not yet transposed the Directive on Privacy and Electronic Communications, including the provisions on unsolicited commercial e-mails, which is part of a new, broader regulatory framework for electronic communications[24]. The European Parliament has recently expressed its concern about this delay[25]. Following the expiry on 31 October 2003 of the deadline to transpose the Directive on Privacy and Electronic Communications, the Commission has opened infringement proceedings in November 2003 for failure to notify transposition measures against a number of Member States[26].

3.1. Introduction

Although legislation will deter some spam, legislation alone will not be sufficient. Effective enforcement of the opt-in must be a priority in all Member States. Next to sufficient staff and resources, this implies adequate enforcement mechanisms, including cross-border mechanisms. Co-operation with non-EU countries is also crucial. Monitoring is also important if only to determine enforcement priorities.

A number of factors seem to influence the effectiveness of enforcement mechanisms:

– the possibility to enforce legislation with effective fines or other penalties. Some regulatory authorities apparently still lack (effective) enforcement powers;

– the nature of complaints mechanisms and remedies available to individuals and companies;

---

23 Proposal for a Council Framework Decision on attacks against information systems, COM(2002) 173 final, 19.4.2002.

24 See also the 9th Report on the Implementation of the Telecommunications Regulatory Package, available at the following URL address: http://europa.eu.int/information_society/topics/ecomm/all_about/implementation_enforcement/annualreports/9threport/index_en.htm

25 The importance of full, effective and timely implementation of the new regulatory framework for electronic communications, including this Directive, has been stressed by the Commission in its Communication "Electronic Communications: the Road to the Knowledge Economy (COM(2003) 65 of 11 February 2003).

26 The letters of formal notice have been sent on the 25th of November 2003 (See IP/03/1663).

– the need for clarity and co-ordination among national authorities in view of their sometimes overlapping duties in this area;

– the level of awareness among users about their rights and how to enforce them. Users need to be given information on where to complain, what will be investigated or not, what types of enforcement action may be taken, and what information they need to provide for the authorities to launch an investigation;

– co-ordination and co-operation among Member States and between Member States and third countries on the national law applicable to given cases;

– the resources available to track down 'spammers' operating within the EU or off shore and hiding their identity including by using others' identity, addresses or servers.

A description of the enforcement provisions applicable to provisions on unsolicited communications has been provided in Section 2.2, above. The way procedures regarding unsolicited commercial e-mails are organised and handled has been quite diverse until now[27]. While the very instrument of an EU Directive implies that Member States keep some margin of manoeuvre in implementing its provisions, effective enforcement is needed whatever method is used.

[27] Note that complaints often also concern related issues e.g. the right of access to personal data and the right to object to data processing.

Diversity in Member States

The enforcement of the provisions on unsolicited commercial communications is not performed by the same authority in all Member States. In a majority, the data protection authority (DPA) enforces the rules in the first place. In other countries however, the national regulatory authority for electronic communications (NRA) performs this task. In yet other countries, enforcement relies mainly on consumer protection authorities (including Consumer Ombudsmen). Often more than one authority would have to be involved in the enforcement of the provisions on unsolicited communications. Moreover, spam in many cases also amounts to misleading or fraudulent practices. (A minority of Member States do not have a consumer protection authority and enforcement is left to consumers associations or consumers themselves) Spamming activities are often linked to data protection infringements such as harvesting, if not cybercrime activities like illegal intrusion into PCs or servers. The corresponding provisions may not be enforced by the same authorities, let alone across borders.

Except in a few Member States, complaints do not necessarily lead to investigation. Pre-infringement contacts are sometimes used, including directions and guidelines to companies, with some success. Sometimes this pre-complaint phase is left to the consumer who should contact the company before filing a complaint. Self-regulation is in place in some countries (e.g. the UK) to organise this first phase of action. In some Member States, industry has some self-regulatory complaints mechanisms already in place. Authorities also often act on their own initiative. Specific entrustment to an administrative authority would normally not preclude direct access to the judicial system.

Not all DPAs have the power to act against legal persons. Nor do all DPAs have (as yet) the possibility to impose sanctions. Those authorities would have to initiate a legal process with the judicial authorities. In France, experience with the e-mailbox has led the DPA to select a few specific cases and refer them to judicial authorities, without much success. In Belgium, a similar experience has led to an exchange of views with the suspected senders and, in cross-border cases, to their referral to EU counterparts or to the US FTC.

A balanced approach including legislation, enforcement and self-regulation is often identified as the most effective enforcement of the opt-in system. Member States are invited to assess the effectiveness of their enforcement mechanism, in particular in the light of the various actions proposed below (see Sections 3.2 to 3.6).

Member States are also invited to develop national strategies to ensure co-operation between data protection authorities (DPAs), consumer protection authorities (CPAs) and national regulatory authorities for eCommunications (NRAs), and to avoid overlap and duplication between the authorities.

To facilitate and co-ordinate exchanges of information and best practices on effective enforcement (e.g. complaints, remedies, penalties, international cooperation 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 also facilitate and co-ordinate work on the other actions identified in this Communication such as: awareness, technical solutions.

Documents drafted following group discussions would generally be submitted to the Communications Committee (COCOM) created under the regulatory framework for electronic communications networks and services and/or to the Article 29 Data Protection Working Party for appropriate action. In particular, the group may draw up benchmarking criteria for the various measures to be proposed.

This online group includes competent national administrations and data protection authorities, and the Commission services. The online group will determine how to ensure the participation of other interested parties.

3.2. Effective remedies and penalties

3.2.1. Discussion

At present, remedies generally include fines or an injunction to cease the unlawful data processing, occasionally including the 'blocking' of the websites involved. In some Member States, 'injunctions to cease' are awarded prior to or concomitantly with fines in case of non-compliance. However, not all authorities have jurisdiction over the complete set of infringements related to spam, neither do they all have the same tools at their disposal. Cases are also often referred to judicial authorities. Not all Member States have judicial sanctions in place for infringements.

Not all Member States provide for remedies and fines/penalties under administrative law, or under criminal law. Criminal sanctions vary, including terms of imprisonment in certain Member States. In addition, there is generally the possibility to claim damages under civil law.

While there is often a distinction between 'light' and 'serious' offences (e.g. massive mailings, misleading or fraudulent advertising and trade practices), penalties themselves vary greatly among Member States.

In many cases, spam activities may also lead to remedies provided under general data protection legislation (e.g., breach of the obligation to notify, of the right of access, of the obligation to appoint a representative in an EU Member State, etc.) or under specific legislation (e.g., misleading advertising, fraudulent marketing, etc.). Prior to the opt-in regime in particular, various legal grounds have been used to tackle certain forms of spam (e.g., bulk e-mail campaigns, illegitimate use of personal data, network disruption, abuse of e-mail accounts, fraud and misinterpretation of contracts).

Generally speaking, judicial redress is not considered as sufficient enforcement. In general, administrative fines can be imposed, by the DPA, CPA and/or the NRA but amounts vary. Member States with no such possibility are generally considering their introduction. Compared to judicial remedies, administrative sanctions seem to be particularly adequate for such a dynamic sector. DPAs, CPAs and NRAs often avail themselves of complementary tools for enforcement. Administrative procedures can be both affordable and speedy (e.g. reportedly within fifty days by the Italian DPA).

3.2.2. Proposed actions

As a prerequisite, the Commission urges those Member States that have not yet transposed the Directive and in particular the provisions on unsolicited communications, to complete this task without further delay. The Commission services are willing to assist Member States if needed.

Member States are invited to assess the effectiveness of their system of remedies and penalties for infringements and create adequate possibilities for victims to claim damages.

Member States and competent authorities with no administrative remedies should consider adopting such remedies against spam, as a tool to ensure a fast, affordable and effective procedure to enforce the opt-in regime.

The Commission will look to confirm that national transposition measures provide for real sanctions in the event of breach of the relevant requirements by market players, including where appropriate financial and criminal penalties.

In this context, the Commission will also investigate how far competent authorities have the required investigation and enforcement powers.

3.3. Complaints mechanisms

3.3.1. Discussion

Effective enforcement implies adequate complaint mechanisms. Some DPAs have set up e-mailboxes to which users can forward unsolicited commercial e-mail and have committed themselves to undertaking action in targeted cases.

Some Member States seem to prefer normal administrative procedures and/or contacts with ISPs, or Computer Emergency Response Teams (CERTs) in case of network disruption. Other Member States favour more traditional procedures (damage claims under civil law/administrative proceedings). Co-regulation or self-regulation is sometimes invoked as better alternatives to direct enforcement measures.

Best Practices

France and Belgium have used dedicated e-mailboxes in late 2002 to receive specific complaints about spam and the results are quite interesting. Reports on these initiatives are available to the public[28]. It is expected that France will run an e-mailbox on a permanent basis under the new rules transposing the Directive on Privacy and Electronic Communications. The Federal Trade Commission (FTC) in the USA operates a similar mailbox and uses the input for prosecution on the basis of existing laws on unfair and deceptive trade practices[29].

Among the advantages of e-mailboxes is the fact that they appear to encourage consumers to report infringements and hence make enforcement of adopted legislation more effective. In addition, they can provide essential statistics about the size and the nature of the problems encountered in a given country or region giving a clear overview which, in turn, gives authorities a valuable tool for setting enforcement priorities or, indeed, adapting them. Moreover, preventive actions can be built on the basis of the knowledge acquired. As an illustration, the CNIL, i.e., the French DPA, has used information gathered during their 'boîte à spams' operation to build preventive information packages targeted at users and at marketeers.

---

28 The report of 24 October 2002 adopted by the 'Commission National Informatique et Libertés' (CNIL), the French DPA is available at the following URL address: http://www.cnil.fr/frame.htm?http://www.cnil.fr/thematic/internet/spam/spam_sommaire.htm The July 2003 report by the 'Commission de Protection de la Vie Privée', the Belgian DPA, can be accessed at the following URL address: http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf

29 See e.g. http://www.ftc.gov/bcp/conline/pubs/online/inbox.pdf Unwanted or deceptive messages can be sent to the following URL address: uce@ftc.gov

The usefulness of an e-mailbox to monitor and measure the scale and scope of spam understandably depends on the ability to investigate the complaints made in a useful and rapid manner.

While there is generally an interest in learning from other Member States' experience with e-mailboxes, only some Member States appear to plan or consider the possibility to use a dedicated e-mailbox. The reasons indicated are generally: the existing possibility to complain by e-mail via, typically, the authority's website; the need for additional dedicated staff and equipment; or the need to change existing legal procedures.

3.3.2. Proposed actions

Member States and competent authorities should assess the effectiveness of their legal system to cope with user complaints and envisage adaptations if needed.

Member States and competent authorities are invited to set up dedicated e-mailboxes, supported by information campaigns.

These dedicated e-mailboxes would have to be designed in a way that enables simple search and analysis for reasons of better understanding of the problem and to set enforcement priorities.

The Commission services will facilitate the sharing of information on e-mailbox experiences.

3.4. Cross-border complaints and co-operation on enforcement inside the EU

3.4.1. Discussion

Dealing with cross-border complaints effectively is part of protecting consumers successfully in this area. It will be very important to ensure that the national complaints mechanisms, whatever their modalities, can be linked to ensure that complaints from users in one Member State regarding messages originating in another Member State will also be dealt with effectively (see 3.5, below for co-operation with third countries).

At present not all Member States have a formal procedure to deal with cross-border complaints. Current solutions include contacts with the relevant authority in another Member State and the possible transfer of the complaint to the relevant authority where the message(s) originate.

Work is being done by DPAs at the European level (including EEA and candidate countries) to exchange information on cross border complaints, by the 'Complaints handling workshop', a group created within the framework of the European Conference of Data Protection Commissioners. The opportunity exists to use it for cross-border complaints related to spam including work on the determination of the law applicable to given cases. At the same time, not all DPAs enforce the provisions on unsolicited communications.

In the area of consumer protection, the Commission has recently proposed a Regulation on consumer protection co-operation establishing a network of consumer protection

public authorities to deal with cross-border problems[30]. It puts in place mutual assistance procedures and provides for in-depth operational co-operation between national authorities. Spam that is misleading or deceptive or breaches other consumer protection rules would be covered by the regime proposed, but not all spam banned by the Directive on Privacy and Electronic Communications. The Regulation is currently under discussion in Council and Parliament.

3.4.2. Proposed actions

Member States and competent authorities are invited to assess the effectiveness of their existing procedures for handling cross-border complaints (e.g. mutual assistance agreements).

Co-ordination among competent national authorities is encouraged. This includes co-ordination and exchanges of information among authorities enforcing the new provisions, and among those and other authorities in charge of specific forms of spam (e.g., fraudulent spam or 'scams', pornographic spam, messages on illegally distributed health-related products).

As regards fraudulent and deceptive spam, the Council and the Parliament are urged to agree on the proposed Regulation on consumer protection co-operation as quickly as possible to ensure that EU consumer protection authorities are fully equipped to deal with misleading and deceptive spam. They are also invited to consider the possible extension of the scope of this Regulation to the Directive on Privacy and Electronic Communications.

Member States are invited to investigate ways of removing existing barriers to information exchange and co-operation and the possibility of requesting action from their counterparts in other Member States. In practical terms it could be useful to have a liaison mechanism (see the DPAs' initiative mentioned above) by which national regulators could cooperate in pursuit of cross-border enforcement. The establishment of a network to support the co-operation could take advantage of existing Commission programmes such as IDA[31].

The Commission intends to facilitate and promote such co-ordination efforts among competent national authorities, in particular through the newly created informal online group on unsolicited commercial communications. The Commission services have started to investigate, together with Member States and national authorities involved with enforcement, what concrete action is needed to improve the handling of cross-border complaints. Discussions with national authorities will continue throughout 2004.

3.5. Co-operation with third countries

3.5.1. Discussion

The new 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). As a consequence, Article 13 of

[30] COM(2003) 443 final.

[31] Information about the IDA programme is available via the following URL address: http://europa.eu.int/comm/enterprise/ida/index.htm

Directive 2002/58/EC establishing the opt-in rule is applicable to all unsolicited commercial communications received on and sent from networks in the EU (and EEA). This implies that such 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. Still it is important since much spam comes from outside the EU.

While a mix of various instruments will be needed, including prevention, filtering techniques, self-regulation, contracts, international co-operation, the present section focuses particularly on international co-operation. The first objective of international co-operation is to promote the adoption of effective legislation in third countries. The second objective is to cooperate with third countries to ensure effective enforcement of the applicable rules.

There is not much experience on enforcement of existing opt-in or opt-out rules for communications originating outside the EU. Besides the fact that spam is a relatively new phenomenon, obstacles often singled out include the difficulty of identifying the senders of such spam or the amount of effort required to do so; the lack of (appropriate) international co-operation mechanisms; and the lack of jurisdiction of some authorities on international matters.

As regards fraudulent and deceptive spam, the Commission's proposal for a Regulation on consumer protection co-operation also provides for co-operation with third countries on enforcement. The Organisation for Economic Co-operation and Development (OECD) adopted in 2003 a Recommendation designed to protect consumers from fraudulent and deceptive commercial practices across borders[32].

3.5.2. Proposed actions

At the multilateral level, some Member States already participate actively in forums such as the OECD, where work on spam has started. Active participation in this work is encouraged in particular as regards the elaboration of solutions at the international level.

The Commission will host an OECD workshop on spam in February 2004 which is intended to produce a better understanding of the problem created by spam and contribute to solutions at the international level. Concrete follow-up actions at OECD level will build on the results of the workshop. The Commission services are discussing these 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.

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 Commission will investigate how best to follow-up the results of the 2003 World Summit in the EU, taking account of the Tunis Summit to be held in 2005.

[32] OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, OECD, 2003.

Member States and competent authorities are also invited to reinforce, or engage in bilateral co-operation with third countries. This includes not only the promotion of effective legislation but also co-operation on enforcement, including police and judicial co-operation where appropriate.

Co-operation is also encouraged between authorities and the private sector, in particular ISPs and ESPs in order to trace back spammers, subject to appropriate legal safeguards.

The Commission services will continue to be active in international fora, including the OECD and the workshop that the Commission will host in Brussels in February 2004. It will also continue to hold bilateral meetings and discussions with third countries, *inter alia* to encourage third countries to take effective action against spam, and in particular the most offensive forms of spam, and to promote co-operation on enforcement

The Commission services have started to investigate, together with Member States and national authorities involved with enforcement, how best to ensure international co-operation, in particular to ensure the handling of complaints concerning spam originating in third countries. This work with national authorities will continue throughout 2004.

3.6. Monitoring

3.6.1. Discussion

In order to evaluate how the opt-in system works in practice and to address specific problems with suitable measures, Member States will need objective and up to date information on trends in spam, user complaints and difficulties encountered by service providers. Sources and type of information would include: trends in the nature of spam, origin and volume of unsolicited commercial e-mail as detected by filtering software providers, service providers and national (regulatory) initiatives; and statistics resulting from the use of a complaints e-mailbox where applicable.

The OECD has started in 2003 to work on the measurement of unsolicited electronic messages at international level and will pursue its work in 2004.

Article 18 of the Directive on Privacy and Electronic Communications provides for a report in 2006 on the application of the Directive and its impact on economic operators and consumers, with specific emphasis on unsolicited communications. In drawing up this report, the Commission will need to seek information from Member States, including relevant statistics.

3.6.2. Proposed actions

Member States should 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 the measurement of unsolicited electronic messages.

The Commission will use the newly created informal online group on unsolicited commercial communications to facilitate and co-ordinate exchanges of information and best practices on trends and statistics on spam.

4. TECHNICAL AND SELF-REGULATORY ACTIONS FOR INDUSTRY

This section on self-regulatory and technical issues covers proposed actions for market players in particular, in areas like: contractual arrangements, codes of conduct, acceptable marketing practices, labels, alternative dispute resolutions mechanisms. It also covers some technical solutions, e.g., filtering, security of servers.

4.1. Effective application of the opt-in regime

4.1.1. Discussion

Combating spam is a matter for all interested parties. Industry can play a specific role since it can by turning the opt-in regime into a day-to-day business practice. Day-to-day practice includes not only terms and conditions for end-users, but also dealings with business partners.

In many cases, better co-ordination through industry associations, and involvement of sector-specific self-regulatory bodies and consumer/user associations is needed, including the involvement of data protection authorities or other competent national authorities.

Best practice

As an illustration, in the Netherlands, starting in 2002, the Electronic Commerce Platform has hosted a platform called 'Basic Principles for Commercial e-Mail' that groups different branches of the industry (Direct Marketing and ISPs) as well as the Dutch Consumers' Association. The intention is to develop practical implementation of the opt-in principle. This practical implementation will be tested with the data protection authority[33].

Contracts can help in the fight against spam, subject to safeguards with respect to individual rights. Many internet service providers (ISPs) and e-mail service providers (ESPs) already include obligations in contracts with their customers prohibiting the use of their services for sending spam. Such ISPs and ESPs already prohibit the sending of unsolicited e-mail, or bulk e-mail, from their e-mail accounts[34].

The concepts as used in previous contracts between ISPs and their customers are likely to be different from those used in the new Directive and subsequent national transposition law.

In terms of customer service, there is also a need for a more pro-active filtering policy by providing information on anti-spam filters, and by providing filtering services or facilities to subscribers as an option.

The same is valid whenever ISPs or mobile operators enter into contracts with third parties and in particular with direct marketeers. This concerns, for instance, not just direct relationships with companies offering 'value added' services. It also includes operators with whom a given service provider has interconnection agreements, as is the case in mobile services.

---

[33] see http://www.ecp.nl/projecten.php#32 .

[34] Such clauses are sometimes based on the need to take all measures to prevent inappropriate usage of their services. Other refer to existing codes of conduct regarding bulk e-mails or, indeed, to self-regulatory principles (e.g. 'netiquette').

The new opt-in regime has also implications on several direct marketing activities, such as:

- the methods for collecting e-mail addresses and other electronic contacts details to the new regime (As noted above, the harvesting of e-mail addresses is incompatible with Community law);

- the adaptation of existing lists;

- the prohibitions on using data without consent and on selling non-compliant lists.

4.1.2. Proposed actions

Industry involvement and self-regulation or, indeed, co-regulation, should be promoted, in particular in areas where legislation and enforcement by public authorities alone may not be sufficient. All interested parties should play their part in this area, including consumer associations and/or users' associations.

Service providers' contractual practices towards subscribers and business partners

Firstly, industry will have in particular to assess the extent to which their existing contracts are compatible with the new rules and, if not, adapt them accordingly.

This concerns adaptation of terms and conditions of subscriber contracts. This is applicable not only to ISPs and ESPs but also to providers of mobile services. As a complementary measure, provision of information on filters and on filtering software or services could be provided as optional customer service (on filtering, see also section 4.3, below). Clauses in contracts with business partners (e.g., mobile interconnection, value-added services) should also reflect opt-in compliant marketing practices and provide for adequate penalties in case of breach.

Direct marketeers' own practices

Secondly, adaptation of direct marketeers' practices to the opt-in regime may be necessary. Direct marketeers could in particular agree on specific, legally compliant methods to collect personal data (e.g., 'double' or 'confirmed' opt-in systems).

Codes of conduct

Thirdly, various initiatives have already been announced by industry associations such as the adaptation or adoption of codes of conduct and the dissemination of good marketing practices[35]. Europe-wide online codes of conduct for direct marketing will be supported by the Commission. Codes of conduct and other self-regulatory initiatives, and contracts must conform to the opt-in rules. Involvement of the competent regulatory authority could be helpful in this regard. It should be recalled in that context that the Article 29 Data Protection Working Party can approve EU-wide codes of conduct (see Article 30 of the 'general' Data Protection Directive 95/46/EC).

As is often the case, effective application of self-regulatory solutions will depend on the structure put in place to oversee respect for the agreed rules, including effective sanctions.

[35] The European Federation of Direct Marketing (FEDMA) has announced a specific online code of conduct for direct marketeers.

Labels

Fourthly, in order to promote greater awareness among users, tools such as labels (e.g. also known as 'trustmarks' or 'webseals') could be used, in particular where trusted third parties supervise and certify the compliance of market players with codes of conduct .

Visible labels can assist users in identifying ISPs, ESPs and other industry players that adhere to EU rules and/or recognised codes of conduct implementing EU rules. They could also help in making filtering systems more efficient.

Labelling of opt-in compliant users' databases could also be envisaged, as well as labelling of opt-in compliant e-mails (e.g. use of the label 'ADV' in the subject line of an email to indicate that it contains advertising).

Labels could also enable recipients to clearly identify such commercial communications in accordance with the Directive on electronic commerce (see Article 6 (a) of Directive 2000/31/EC; see also section 2, above)

4.2. Alternative dispute resolution (ADR) mechanisms

4.2.1. Discussion

For privacy infringements like sending unsolicited e-mail, an out-of-court redress mechanism may be useful in achieving a higher level of compliance with the new rules. Various initiatives have been launched at national and EU level for alternative dispute resolution (ADR) mechanisms to deal with disputes in relation to online transactions and communications. The Commission has adopted Recommendations on ADR in 1998 and 2001, thereby setting out principles to be applied to such systems. Several initiatives are underway regarding consumer protection-related ADR systems (e.g. EEJ-NET)[36]. Article 17 of the Directive on electronic commerce also encourages the development of such mechanisms.

Out-of court redress mechanisms exist in some countries, sometimes established by legislation, though they vary in many respects, such as origin (branch-specific e.g., direct marketing, e-mail marketing), 'jurisdiction', powers and sanctions (e.g., damage claims), involvement of specific authorities (e.g., DPAs, advertising standards bodies) etc.

For those mechanisms to be sufficiently effective, certain conditions need to be met, such as, how they are organised and promoted, and how is compliance with rulings ensured. Setting them up would also require co-operation between authorities and industry.

4.2.2. Proposed actions

The creation and use of effective self-regulatory complaints mechanisms and alternative dispute resolution mechanisms (ADR) is encouraged, building on existing initiatives whenever possible (e.g. EEJ-NET). They could be particularly useful with respect to cases where international co-operation would be more difficult to achieve.

[36] More information is available at: http://europa.eu.int/comm/consumers/redress/out_of_court/index_en.htm

4.3. Technical issues

4.3.1. Discussion

Different solutions are used to counter spam on the technical front. The Internet community (e.g., RIPE, IETF) has also been taking the problem of spam seriously37. Longer-term initiatives, such as new technical standards for e-mail, are not covered in the present document. ISPs and ESPs often block incoming mail from servers that are used for sending spam (black listing) until the source of the spam is identified and prevented from using the server. In addition, filtering software can be employed by individual users within their own terminal equipment or by electronic communications service providers within their servers.

However not all filtering practices and techniques offer the same level of user control. Nor do they offer the same guarantees for data protection and privacy, such as respect for the confidentiality of communications. They may also not yet be adapted to the new opt-in regime applicable in EU countries for marketing communications (prior consent-based, marketing related, bulk and non-bulk). Also, more differentiation between legitimate marketing (e.g. opt-in compliant) and unsolicited commercial communications may allow the development of more effective filtering software.

While the new legal provisions on unsolicited commercial e-mail provide additional safeguards for the user and greater security for service providers to undertake action on request against 'spammers', filtering may occasionally block legitimate e-mail ('false positive') or allow spam to get through ('false negatives'). In some cases, this can create a risk that either a sender or an intended addressee undertakes legal action against an ISP/ESP. Some ISPs/ESPs therefore offer filtering as an optional service to their users and require permission for activating it.

Although it is beyond the scope of this Communication to address them, other issues, such as filtering versus freedom of expression and filtering versus the contractual obligation of ISPs/ESPs to transmit email messages to their clients' customers, are also presented by the use of filtering techniques to combat spam.

As regards filtering in mobile services, the different business model environment for mobile services compared to fixed internet services may justify different solutions. In particular, the former model would normally include per-message delivery charges, which make spam more costly. However, some new services entail charging based on retrieval, and this means that spam increases the costs for the recipient. In addition, e-mail can now be delivered to mobile terminals. Filters and viewing facilities could then be provided to subscribers to manage mobile spam.

Attention is also needed on open relays. In short, open relays are SMTP servers that can be used for relaying messages that are sent by users other than local users of the server. In the past, most relays were open. However, when relays are open, they can be used by

---

37 For instance, the RIPE (Réseaux IP Européens) Anti-spam Working Group has been active since 1998 (see: The document "Good Practice for combating Unsolicited Bulk Email" can be found on the RIPE website (see: http://www.ripe.net). More recently, the IRTF (Internet Research Task Force) has set up an Anti-Spam Research Group (see: http://www.irtf.org/charters/asrg.html). This group may develop certain technologies that could serve as a starting point for standardisation efforts within the IETF (Internet Engineering Task Force).

spammers to send unsolicited communications quite easily. Simple preventive measures would reduce the possibilities for such abuse. The same is true for open proxies, which are servers that run software allowing direct interaction with the Internet.

4.3.2. Proposed actions

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 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.

Users should be given the opportunity to manage the way in which incoming spam is handled, according to individual needs. 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.

Filtering companies should cooperate with interested parties to develop techniques recognising marketing e-mails corresponding to accepted marketing practices under Community law, including webseals, labels, etc.

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.

5. AWARENESS ACTIONS

This section on awareness issues covers proposed actions in areas like prevention, consumer awareness, reporting.

5.1. Discussion

EU Member States should have transposed the new opt-in regime for unsolicited e-mail into national law by 31 October 2003 at the latest. While this new approach has had a fair amount of publicity in the press, some uncertainty may remain among market players and citizens about what the 'opt-in' actually means in practice[38].

This new approach is based on user empowerment to consent or not to receiving commercial communications. To enable this however, they must be aware of the basic rules applicable to unsolicited communications and where to report problems.

[38] Background information on the rules applicable to unsolicited communications under Directive 2002/58/EC is available at the following URL address: http://europa.eu.int/information_society/topics/ecomm/all_about/todays_framework/privacy_protection/index_en.htm#unsolicited

Best practice

The UK Information Commissioner (the UK data protection authority) has published, a few weeks before the entry into force of the new regulations implementing the Directive, a guidance document explaining the new UK rules, with a specific part on marketing by electronic means. The Information Commission has also announced that complaints forms would be available online and from their offices when the rules come into force, setting out the information likely to be needed[39].

Also users must understand the risks of sharing their personal data over the Internet (e.g. leaving them when visiting websites, Usenet) and should adapt their behaviour accordingly.

Finally, they need to know what filtering software is on the market and what service and software providers (e.g. ISPs, ESPs) can do for them.

Best practice

The 'Commission National Informatique et Libertés' ('CNIL'), i.e., the French Data Protection Authority has posted a substantial information package on its website relating to various aspects of spam: the results of its e-mailbox experience and the cases referred to judicial authorities (see below), basic guidance on how to prevent spam, information on how to report spam, references of users' associations active in this area, etc.

While awareness-raising activities concerning the new opt-in regime have been undertaken, or are envisaged, in most Member States, they differ widely in terms of timing, the nature of information provided, the target audience and the parties involved. Some Member States however wait until their laws are in place. Public consultation on the implementation of Directive 2002/58/EC has contributed to a certain degree of awareness whenever it has been organised.

Various authorities can be responsible for these activities depending on their respective powers in a given Member State (e.g. DPAs, NRAs, CPAs, ombudsmen). Co-ordination among the various competent authorities does not (yet) exist in all Member States. Ministries appear to be involved in some Member States. Industry associations are often involved. Sometimes consumer or user associations are also taking part in these activities.

Some parts of the industry as well have undertaken awareness raising activities at national, EU or global level, although here again, these activities can differ widely. These include:

– practical guides to direct marketeers, or campaigns directed at the communications sector in particular;
– general guidance to customers on codes of conduct, complaint mechanisms and filtering;
– platform/working groups to develop best practices for commercial communications.

---

39 See: http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_200258ec.html#guidance

5.2. Proposed actions

In order to achieve a high level of understanding about the new do's and don'ts with regard to commercial e-mail, broad and sustained action is needed in the short term in all Member States on both prevention and enforcement. Practical information on prevention, acceptable marketing practices, and on technical and legal solutions available to users should be provided.

All parties are invited to play their role in awareness raising activities, from Member States and competent authorities, through businesses, to consumers/user associations. Member States and competent authorities not yet doing so are invited to launch or support campaigns in early 2004.

In particular as regards the nature of information provided, activities targeted at businesses and/or consumers should include:

- Ensuring 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.

The Safer Internet programme and spam

The European Commission has published a call for proposals under the Safer Internet programme where projects could be proposed to deal with spam under various actions, e.g. on awareness. Projects selected under the first evaluation of this call could start in May 2004.

The Commission is currently preparing a proposal for a follow-up programme, Safer Internet *plus*, which will propose funding of further measures to deal with illegal and harmful content and unwanted content such as spam.

http://www.europa.eu.int/information_society/programmes/iap/call/index_en.htm

These actions should reach the following target groups:
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.

Awareness activities should be carried out through different channels (not only web-based), 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.

Actions listed above should also refer to effective industry codes of conduct, complaints mechanisms, labels (e.g. 'trustmarks') and certification schemes where available.

The Commission services already provides information on the basics of opt-in on the EUROPA website[40]. 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.

CONCLUSION

Spam is one of the most significant challenges facing the Internet today. Addressing spam however requires action on various fronts, involving not only effective enforcement and international co-operation, but also self-regulatory and technical solutions by industry, and consumer awareness. The series of actions identified in the present Communication has been summarised in the table below.

While the Commission will support these efforts as much as possible, it will primarily be for EU Member States and competent authorities, industry, and consumers and users of the Internet and electronic communications services to play their role, both at the national and international level.

Integrated and parallel implementation of the series of actions identified in this Communication, which have the broad support of interested parties, can contribute to greatly reducing the amount of spam that is currently compromising the benefits of e-mail and other electronic communications for our societies and our economies.

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

[40] http://europa.eu.int/information_society/topics/ecomm/highlights/current_spotlights/spam/index_en.htm

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.