The content of this book has been developed with support of CCSA.

Publisher:
CCD COE Publications
Filtri Tee 12
10132 Tallinn
Estonia
Tel: +372 717 6800
Fax: +372 717 6308
E-mail: publications@ccdcoe.org
www.ccdcoe.org

Printed By: EVG Print
Design & Layout: Marko Söönurm

ENEKEN TIKK

FRAMEWORKS

FOR INTERNATIONAL CYBER SECURITY

2010

PREFACE

The first edition of the Frameworks for International Cyber Security is a response to the growing demand on the international cyber security community to keep pace with cyber threats, whether mirrored in threat assessments or brought to attention by real-life incidents. The edition represents a compilation of cyber security legal and policy instruments adopted by the Council of Europe, the European Union, the Group of Eight, the International Telecommunication Union, the Organization for Economic Co-Operation and Development, the Organization for Cooperation and Security in Europe and the United Nations that provide various tools and approaches to handle the threats against modern information societies.

In this time where we are increasingly affected by international principles and rules of cyber security and need to ensure respect for their implementation on national level, this handbook aims to start a series of reference materials for those who are tasked with the legislative, policy-designing and decision-preparing tasks related to cyber incident handling. I intend to complement this series with editions reflecting more regional approaches to cyber security as well as compilations of recently developed national cyber security strategies, cyber security related case law and national legislative best practices.

This edition is not an exhaustive set of existing international instruments; it covers just a selection of international organizations – mainly those that are relevant to the European-American players on the security field. Also, it only contains instruments that are made available to the public. Yet, triggered by my personal interest towards how many legal and policy instruments are potentially influencing national cyber security arrangements, it should be a rather comprehensive representation of what currently exists in international law to safeguard cyber security.

I look forward to updating this material and am therefore thankful in advance to individuals and organizations for their feedback and comments that help to develop the online version and possibly a paperback version of this handbook.

I want to thank Anna-Maria, Liis and Kadri for their help and insights and support. Also, I am most thankful to the Cooperative Cyber Defence Centre of Excellence and Cyber Conflict Studies Association for letting me invest time and effort in this study. Anyone who would like to contribute to the development project of this reference material is more than welcome to join the team!

Tallinn, April 2010

Eneken Tikk

Contents

COUNCIL OF EUROPE

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981)

Preamble

The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:

CHAPTER I
GENERAL PROVISIONS

Article 1
Object and purpose

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Article 2
Definitions

For the purposes of this convention:

a. "personal data" means any information relating to an identified or identifiable individual ("data subject");

b. "automated data file" means any set of data undergoing automatic processing;

c. "automatic processing" includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination;

d. "controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.

Article 3
Scope

1. The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.

2. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:

   a. that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law;

   b. that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;

   c. that it will also apply this convention to personal data files which are not processed automatically.

3. Any State which has extended the scope of this convention by any of the declarations provided for in sub-paragraph 2.b or c above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.

4. Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2.a above may not claim the application of this convention to such categories by a Party which has not excluded them.

5. Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraphs 2b and c above may not claim the application of this convention on these points with respect to a Party which has made such extensions.

6. The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

CHAPTER II
BASIC PRINCIPLES FOR DATA PROTECTION

Article 4
Duties of the Parties

1. Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

2. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

Article 5
Quality of data

Personal data undergoing automatic processing shall be:

a. obtained and processed fairly and lawfully;

b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are stored;

d. accurate and, where necessary, kept up to date;

e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6
Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7
Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Article 8
Additional safeguards for the data subject

Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Article 9
Exceptions and restrictions

1. No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

   a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

   b. protecting the data subject or the rights and freedoms of others.

3. Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientif-ic research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10
Sanctions and remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

Article 11
Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this convention.

CHAPTER III
TRANSBORDER DATA FLOWS

Article 12
Transborder flows of personal data and domestic law

1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:

   a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;

   b. when the transfer is made from its territory to the territory of a non Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

CHAPTER IV
MUTUAL ASSISTANCE

Article 13
Co-operation between Parties

1. The Parties agree to render each other mutual assistance in order to implement this convention.

2. For that purpose:

   a. each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;

   b. each Party which has designated more than one authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority.

3. An authority designated by a Party shall at the request of an authority designated by another Party:

   a. furnish information on its law and administrative practice in the field of data protection;

   b. take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.

Article 14
Assistance to data subjects resident abroad

1. Each Party shall assist any person resident

abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention.

2. When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.

3. The request for assistance shall contain all the necessary particulars, relating inter alia to:

   a. the name, address and any other relevant particulars identifying the person making the request;

   b. the automated personal data file to which the request pertains, or its controller;

   c. the purpose of the request.

Article 15
Safeguards concerning assistance rendered by designated authorities

1. An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.

2. Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.

3. In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned.

Article 16
Refusal of requests for assistance

A designated authority to which a request for assistance is addressed under Articles 13 or 14 of this convention may not refuse to comply with it unless:

a. the request is not compatible with the powers in the field of data protection of the authorities responsible for replying;

b. the request does not comply with the provisions of this convention;

c. compliance with the request would be incompatible with the sovereignty, security or public policy (ordre public) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party.

Article 17
Costs and procedures of assistance

1. Mutual assistance which the Parties render each other under Article 13 and assistance they render to data subjects abroad under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party which has designated the authority making the request for assistance.

2. The data subject may not be charged costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents of that Party.

3. Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

CHAPTER V
CONSULTATIVE COMMITTEE

Article 18
Composition of the committee

1. A Consultative Committee shall be set up after the entry into force of this convention.

2. Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the convention shall have the right to be represented on the committee by an observer.

3. The Consultative Committee may, by unanimous decision, invite any non-member State of the Council of Europe which is not a Party to the convention to be represented by an observer at a given meeting.

Article 19
Functions of the committee

The Consultative Committee:

a. may make proposals with a view to facilitating or improving the application of the convention;

b. may make proposals for amendment of this convention in accordance with Article 21;

c. shall formulate its opinion on any proposal for amendment of this convention which is referred to it in accordance with Article 21, paragraph 3;

d. may, at the request of a Party, express an opinion on any question concerning the application of this convention.

Article 20
Procedure

1. The Consultative Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this convention. It shall subsequently meet at least once every two years and in any case when one-third of the representatives of the Parties request its convocation.

2. A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.

3. After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the convention.

4. Subject to the provisions of this convention, the Consultative Committee shall draw up its own Rules of Procedure.

CHAPTER VI
AMENDMENTS

Article 21
Amendments

1. Amendments to this convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Consultative Committee.

2. Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe and to every non-member State which has acceded to or has been invited to accede to this convention in accordance with the provisions of Article 23.

3. Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.

4. The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.

5. The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.

6. Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

CHAPTER VII
FINAL CLAUSES

Article 22
Entry into force

1. This convention shall be open for signature by the member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

2. This convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the convention in accordance with the provisions of the preceding paragraph.

3. In respect of any member State which subsequently expresses its consent to be bound by it, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of ratification, acceptance or approval.

Article 23
Accession by non member States

1. After the entry into force of this convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention

by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee.

2. In respect of any acceding State, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 24
Territorial clause

1. Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this convention shall apply.

2. Any State may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this convention to any other territory specified in the declaration. In respect of such territory the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

Article 25
Reservations

No reservation may be made in respect of the provisions of this convention.

Article 26
Denunciation

1. Any Party may at any time denounce this convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

Article 27
Notifications

The Secretary General of the Council of Europe shall notify the member States of the Council and any State which has acceded to this convention of:

a. any signature;

b. the deposit of any instrument of ratification, acceptance, approval or accession;

c. any date of entry into force of this convention in accordance with Articles 22, 23 and 24;

d. any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Strasbourg, the 28th day of January 1981, in English and in French, both texts being equally authoritative, in a single copy which shall remain deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe and to any State invited to accede to this Convention.

Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows (2001)

Preamble

The Parties to this additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature in Strasbourg on 28 January 1981 (hereafter referred to as "the Convention");

Convinced that supervisory authorities, exercising their functions in complete independence, are an element of the effective protection of individuals with regard to the processing of personal data;

Considering the importance of the flow of information between peoples;

Considering that, with the increase in exchanges of personal data across national borders, it is necessary to ensure the effective protection of human rights and fundamental freedoms, and in particular the right to privacy, in relation to such exchanges of personal data,

Have agreed as follows:

Article 1
Supervisory authorities

1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.

2.

   a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

   b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.

3. The supervisory authorities shall exercise their functions in complete independence.

4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.

5. In accordance with the provisions of Chapter IV, and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

Article 2
Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention

1. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.

2. By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data :

   a. if domestic law provides for it because of :

      - specific interests of the data subject, or
      - legitimate prevailing interests, especially important public interests, or

   b. if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.

Article 3
Final provisions

1. The provisions of Articles 1 and 2 of this Protocol shall be regarded by the Parties as additional articles to the Convention and all the provisions of the Convention shall apply accordingly.

2. This Protocol shall be open for signature by States Signatories to the Convention. After acceding to the Convention under the conditions

provided by it, the European Communities may sign this Protocol. This Protocol is subject to ratification, acceptance or approval. A Signatory to this Protocol may not ratify, accept or approve it unless it has previously or simultaneously ratified, accepted or approved the Convention or has acceded to it. Instruments of ratification, acceptance or approval of this Protocol shall be deposited with the Secretary General of the Council of Europe.

3.

a. This Protocol shall enter into force on the first day of the month following the expiry of a period of three months after the date on which five of its Signatories have expressed their consent to be bound by the Protocol in accordance with the provisions of paragraph 2 of Article 3.

b. In respect of any Signatory to this Protocol which subsequently expresses its consent to be bound by it, the Protocol shall enter into force on the first day of the month following the expiry of a period of three months after the date of deposit of the instrument of ratification, acceptance or approval.

4.

a. After the entry into force of this Protocol, any State which has acceded to the Convention may also accede to the Protocol.

b. Accession shall be effected by the deposit with the Secretary General of the Council of Europe of an instrument of accession, which shall take effect on the first day of the month following the expiry of a period of three months after the date of its deposit.

5.

a. Any Party may at any time denounce this Protocol by means of a notification addressed to the Secretary General of the Council of Europe.

b. Such denunciation shall become effective on the first day of the month following the expiry of a period of three months after the date of receipt of such notification by the Secretary General.

6. The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the European Communities and any other State which has acceded to this Protocol of:

a. any signature;

b. the deposit of any instrument of ratification, acceptance or approval;

c. any date of entry into force of this Protocol in accordance with Article 3;

d. any other act, notification or communication relating to this Protocol.

In witness whereof the undersigned, being duly authorised thereto, have signed this Protocol.

Done at Strasbourg, this 8th day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, the European Communities and any State invited to accede to the Convention.

Convention on Information and Legal Co-operation Concerning "Information Society Services" (2001)

Preamble

The Parties to this Convention, signatories hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members for the purpose of safeguarding and realising the ideals and principles which are their common heritage;

Noting the continued development of information and communication technology and the numerous national initiatives and their impact at a European and international level;

Recognising the cross-border nature of interactive services that are diffused on-line by new means of electronic communication and their growing importance in facilitating the economic, social and cultural progress of the Council of Europe member States;

Recalling the system established by the legislation of the European Community for the exchange of the texts of draft domestic regulations concerning "Information Society Services";

Noting the need for all Council of Europe member States to be kept regularly informed of legislative developments on "Information Society Services" at a Pan-European level and, where necessary, to have the possibility to discuss and exchange information and ideas regarding these developments;

Agreeing on the desirability to provide a legal framework to enable member States of the Council of Europe to exchange, where practicable by electronic means, texts of draft domestic regulations aimed specifically at "Information Society Services",

Have agreed as follows:

Article 1
Object and scope of application

1. In accordance with the provisions of this Convention, the Parties shall exchange texts, where practicable by electronic means, of draft domestic regulations aimed specifically at "Information Society Services" and shall co-operate in the functioning of the information and legal co-operation system set up under the Convention.
2. This Convention shall not apply:
   a. to domestic regulations which are exempted from prior notification by virtue of European Community legislation (hereinafter referred to as "Community law"), or
   b. where a notification has to be made to comply with other international agreements.
3. This Convention shall not apply :
   a. to radio broadcasting services;
   b. to television programme services covered by the European Convention on Transfrontier Television, opened for signature in Strasbourg on 5 May 1989 (ETS No. 132), as amended by the Protocol of 1 October 1998 (ETS No. 171);
   c. to domestic regulations relating to matters which are covered by European Community legislation or international agreements in the fields of telecommunications services and financial services.

Article 2
Definitions

For the purposes of this Convention

a. "Information Society Services" means any service, normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services;
b. "domestic regulations" means legal texts concerning the compliance with requirements of a general nature relating to the taking up and pursuit of service activities within the meaning of paragraph a of this article, in particular provisions concerning the service provider, the services and the recipient of services, excluding any rules which are not specifically aimed at the Information Society Services.

Article 3
Receiving and transmitting authorities

Each Party shall designate an authority that is in charge of transmitting and receiving, where practicable by electronic means, draft domestic regulations aimed specifically at "Information Society Services" as well as any other documents pertaining to the functioning of the present Convention.

Article 4
Procedure

1. Each Party shall transmit, where practicable

by electronic means, to the Secretary General of the Council of Europe the texts of draft domestic regulations which are aimed specifically at "Information Society Services" and which are at a stage of preparation in which it is still possible for them to be substantially amended, as well as a short summary of these texts in English or French. The Parties shall communicate the draft again under the above conditions if they make changes to the draft that have the effect of significantly altering its scope, shortening the timetable originally envisaged for implementation, adding specifications or requirements, or making the latter more restrictive.

2. Upon receipt of the texts of the draft domestic regulations and summaries under paragraph 1 above or paragraph 6 below, the Secretary General of the Council of Europe shall transmit them, where practicable by electronic means, to the authority of each Party.

3. Upon receipt of the texts and summaries under paragraph 2 above, each Party may transmit, where practicable by electronic means, observations on the texts of the draft domestic regulations in English or French to the Secretary General of the Council of Europe and to the Party concerned.

4. A Party receiving the observations under paragraph 3 above shall endeavour to take them into account as far as possible when preparing new domestic regulations.

5. Paragraphs 1 to 4 above shall not apply:

   a. in cases where, for urgent reasons, occasioned by serious and unforeseeable circumstances relating to the protection of public health or safety, the protection of animals or the preservation of plants, and public policy, notably the protection of minors, a Party is obliged to prepare technical regulations in a very short space of time in order to enact and introduce them immediately without any consultations being possible;

   b. in cases where for urgent reasons occasioned by serious circumstances relating to the protection of the security and the integrity of the financial system, notably the protection of depositors, investors and insured persons, a Party is obliged to enact and to implement rules on financial services immediately; in the cases mentioned in subparagraphs a and b, the Party shall give reasons to the Secretary General of the Council of Europe for the urgency of the measures in question;

   c. to domestic regulations enacted by or for regulated markets or by or for other markets or bodies carrying out clearing or settlement functions for those markets.

6. Each Party which finalises any domestic regulations aimed specifically at "Information Society Services" shall transmit the definitive text to the Secretary General of the Council of Europe without delay and where practicable by electronic means.

7. Upon receipt of the texts of the adopted domestic regulations under paragraph 6 above, the Secretary General of the Council of Europe shall make them available, where practicable by electronic means, and shall keep this information in a single database within the Council of Europe.

Article 5
Declarations

The authorities referred to in Article 3 shall be designated by means of a declaration addressed to the Secretary General of the Council of Europe when the State concerned or the European Community becomes a Party to the present Convention in accordance with the provisions of Articles 8 and 9. Any change shall likewise be declared to the Secretary General of the Council of Europe.

Article 6
Relationship to other instruments and agreements

1. This Convention shall not affect any international instrument which is binding on the Parties and which contains provisions on matters governed by this Convention.

2. The European Community shall equally fulfil the obligation to notify the texts transmitted to it by its member States in pursuance of the provisions of paragraph 1 of Article 4, and shall transmit to them the observations received by the other Parties, in pursuance of the provisions of paragraph 3 of Article 4.

Article 7
Amendments to Article 1 of the Convention concerning excluded matters

1. Any amendment to Article 1, paragraph 3 of this Convention proposed by a Party shall be communicated to the Secretary General of the

Council of Europe who shall forward the communication to the European Committee on Legal Co-operation (CDCJ).

2. The proposed amendment shall be examined by the Parties, which may adopt it by a two-thirds majority of the votes cast. The text adopted shall be forwarded to the Parties. The European Community shall have the same number of votes as the number of its member States.

3. On the first day of the month following the expiration of a period of four months after its adoption by the Parties, unless the Parties have notified objections by one-third of the votes cast, any amendment shall enter into force for those Parties which have not notified objection.

4. A Party which has notified an objection in pursuance of the provisions of paragraph 3 of Article 7 may subsequently withdraw it in whole or in part. Such withdrawal shall be made by means of a notification addressed to the Secretary General of the Council of Europe and shall become effective as from the date of its receipt.

Article 8
Signature and entry into force

1. This Convention shall be open for signature by the member States of the Council of Europe, the non-member States which have participated in its elaboration and the European Community. Such States and the European Community may express their consent to be bound by:

   a. signature without reservation as to ratification, acceptance or approval, or

   b. signature subject to ratification, acceptance or approval, followed by ratification, acceptance or approval.

2. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five signatories, of which at least one is not a member State of the European Economic Area, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraph 1.

4. In respect of any signatory which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of their consent to be bound by the Convention in accordance with the provisions of paragraph 2.

Article 9
Accession to the Convention

1. After the entry into force of the present Convention, the Committee of Ministers of the Council of Europe, after consulting the Parties to the Convention, may invite any non-member State of the Council which has not participated in its elaboration to accede to this Convention, by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Parties entitled to sit on the Committee.

2. In respect of any State acceding to it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 10
Reservations

No reservation may be made in respect of any provision of this Convention.

Article 11
Territorial application

1. Any State or the European Community may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any Party may, at any later date, by declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory or territories specified in the declaration and for whose international relations it is responsible or on whose behalf it is authorised to give undertakings. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

3. Any declaration made in pursuance of the preceding paragraph may, in respect of any territory mentioned in such declaration, be withdrawn by means of a notification addressed to

the Secretary General of the Council of Europe. Such withdrawal shall take effect on the first day of the month following the expiration of a period of three months after the date of receipt by the Secretary General of the Council of Europe of the notification.

Article 12
Denunciation

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.
2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 13
Notification

The Secretary General of the Council of Europe shall notify the member States of the Council and any other signatories and Parties to this Convention of:

a. any signature;
b. the deposit of any instrument of ratification, acceptance, approval or accession;
c. any declaration made in pursuance of the provisions of Article 5;
d. any notification received in pursuance of the provisions of Article 7;
e. any date of entry into force of this Convention, in accordance with Articles 8, 9 and 11;
f. any declaration received in pursuance of the provisions of paragraphs 2 and 3 of Article 11;
g. any notification received in pursuance of the provision of paragraph 1 of Article 12;
h. any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Moscow, this 4th day of October 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, to the European Community, as well as to any State invited to accede to it.

Convention on Cybercrime (2001)

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to

bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

CHAPTER I
USE OF TERMS

Article 1
Definitions

For the purposes of this Convention:

a. "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c. "service provider" means:

   (i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

   (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service;

d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

CHAPTER II
MEASURES TO BE TAKEN AT THE NATIONAL LEVEL

SECTION 1
SUBSTANTIVE CRIMINAL LAW

TITLE 1
OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND SYSTEMS

Article 2
Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3
Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4
Data interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5
System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6
Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

   a. the production, sale, procurement for use, import, distribution or otherwise making available of:

      (i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

      (ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

   b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

TITLE 2
COMPUTER-RELATED OFFENCES

Article 7
Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8
Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a. any input, alteration, deletion or suppression of computer data;

b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

TITLE 3
CONTENT-RELATED OFFENCES

Article 9
Offences related to child pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

   a. producing child pornography for the purpose of its distribution through a computer system;

b. offering or making available child pornography through a computer system;

c. distributing or transmitting child pornography through a computer system;

d. procuring child pornography through a computer system for oneself or for another person;

e. possessing child pornography in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a. a minor engaged in sexually explicit conduct;

b. a person appearing to be a minor engaged in sexually explicit conduct;

c. realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

TITLE 4
OFFENCES RELATED TO INFRINGEMENTS OF COPYRIGHT AND RELATED RIGHTS

Article 10
Offences related to infringements of copyright and related rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

TITLE 5
ANCILLARY LIABILITY AND SANCTIONS

Article 11
Attempt and aiding or abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12
Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this

Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a. a power of representation of the legal person;

b. an authority to take decisions on behalf of the legal person;

c. an authority to exercise control within the legal person.

2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13
Sanctions and measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

SECTION 2
PROCEDURAL LAW

TITLE 1
COMMON PROVISIONS

Article 14 – Scope of procedural provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a. the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b. other criminal offences committed by means of a computer system; and

c. the collection of evidence in electronic form of a criminal offence.

3.

a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b. Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

(i) is being operated for the benefit of a closed group of users, and

(ii) does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15
Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers

and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

TITLE 2
EXPEDITED PRESERVATION OF STORED COMPUTER DATA

Article 16
Expedited preservation of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17
Expedited preservation and partial disclosure of traffic data

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

   a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

   b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

TITLE 3
PRODUCTION ORDER

Article 18
Production order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

   a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

   b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

   a. the type of communication service used, the technical provisions taken thereto and the period of service;

   b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

   c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

TITLE 4
SEARCH AND SEIZURE OF STORED COMPUTER DATA

Article 19
Search and seizure of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

   a. a computer system or part of it and computer data stored therein; and

   b. a computer-data storage medium in which computer data may be stored in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

   a. seize or similarly secure a computer system or part of it or a computer-data storage medium;

   b. make and retain a copy of those computer data;

   c. maintain the integrity of the relevant stored computer data;

   d. render inaccessible or remove those computer data in the accessed computer system.

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

TITLE 5
REAL-TIME COLLECTION OF COMPUTER DATA

Article 20
Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

   a. collect or record through the application of technical means on the territory of that Party, and

   b. compel a service provider, within its existing technical capability:

      (i) to collect or record through the application of technical means on the territory of that Party; or

      (ii) to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may

instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21
Interception of content data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

   a. collect or record through the application of technical means on the territory of that Party, and

   b. compel a service provider, within its existing technical capability:

      (i) to collect or record through the application of technical means on the territory of that Party, or

      (ii) to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

SECTION 3
JURISDICTION

Article 22
Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

   a. in its territory; or

   b. on board a ship flying the flag of that Party; or

   c. on board an aircraft registered under the laws of that Party; or

   d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

CHAPTER III INTERNATIONAL CO-OPERATION

SECTION 1 GENERAL PRINCIPLES

TITLE 1 GENERAL PRINCIPLES RELATING TO INTERNATIONAL CO-OPERATION

Article 23
General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

TITLE 2 PRINCIPLES RELATING TO EXTRADITION

Article 24
Extradition

1.

a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7.

a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

TITLE 3
GENERAL PRINCIPLES RELATING TO MUTUAL ASSISTANCE

Article 25
General principles relating to mutual assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26
Spontaneous information

1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

TITLE 4
PROCEDURES PERTAINING TO MUTUAL ASSISTANCE REQUESTS IN THE ABSENCE OF APPLICABLE INTERNATIONAL AGREEMENTS

Article 27
Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2.

   a. Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

   b. The central authorities shall communicate directly with each other;

c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3. Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4. The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b. it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9.

a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c. Where a request is made pursuant to subparagraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28
Confidentiality and limitation on use

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a. kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b. not used for investigations or proceedings other than those stated in the request.

3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4. Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

SECTION 2
SPECIFIC PROVISIONS

TITLE 1
MUTUAL ASSISTANCE REGARDING PROVISIONAL MEASURES

Article 29
Expedited preservation of stored computer data

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2. A request for preservation made under paragraph 1 shall specify:

a. the authority seeking the preservation;

b. the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c. the stored computer data to be preserved and its relationship to the offence;

d. any available information identifying the custodian of the stored computer data or the location of the computer system;

e. the necessity of the preservation; and

f. that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5. In addition, a request for preservation may only be refused if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

6. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30
Expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2. Disclosure of traffic data under paragraph 1 may only be withheld if:

   a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

   b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

TITLE 2
MUTUAL ASSISTANCE REGARDING INVESTIGATIVE POWERS

Article 31
Mutual assistance regarding accessing of stored computer data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

   The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

   The request shall be responded to on an expedited basis where:

   a. there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

   b. the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32
Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33
Mutual assistance in the real-time collection of traffic data

1. The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34
Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

TITLE 3
24/7 NETWORK

Article 35
24/7 Network

1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data,

or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a. the provision of technical advice;

b. the preservation of data pursuant to Articles 29 and 30;

c. the collection of evidence, the provision of legal information, and locating of suspects.

2.

a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

CHAPTER IV
FINAL PROVISIONS

Article 36
Signature and entry into force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37
Accession to the Convention

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38
Territorial application

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month

following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39
Effects of the Convention

1. The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:
   - the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
   - the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
   - the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).
2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.
3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40
Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41
Federal clause

1. A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.
2. When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.
3. With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42
Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43
Status and withdrawal of reservations

1. A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.
2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation,

in whole or in part, as soon as circumstances so permit.

3. The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44
Amendments

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45
Settlement of disputes

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46
Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

   a. the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

   b. the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

   c. consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47
Denunciation

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary

General.

Article 48
Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a. any signature;

b. the deposit of any instrument of ratification, acceptance, approval or accession;

c. any date of entry into force of this Convention in accordance with Articles 36 and 37;

d. any declaration made under Article 40 or reservation made in accordance with Article 42;

e. any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (2002)

The member states of the Council of Europe and the other States to the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, signatory hereto;

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recalling that all human beings are born free and equal in dignity and rights;

Stressing the need to secure a full and effective implementation of all human rights without any discrimination or distinction, as enshrined in European and other international instruments;

Convinced that acts of a racist and xenophobic nature constitute a violation of human rights and a threat to the rule of law and democratic stability;

Considering that national and international law need to provide adequate legal responses to propaganda of a racist and xenophobic nature through computer systems;

Aware of the fact that propaganda to such acts is often subject to criminalisation in national legislation;

Having regard to the Convention on Cybercrime, which provides for modern and flexible means of international co-operation and convinced of the need to harmonise substantive law provisions concerning the fight against racist and xenophobic propaganda;

Aware that computer systems offer an unprecedented means of facilitating freedom of expression and communication around the globe;

Recognising that freedom of expression constitutes one of the essential foundations of a democratic society, and is one of the basic conditions for its progress and for the development of every human being;

Concerned, however, by the risk of misuse or abuse of such computer systems to disseminate racist and

xenophobic propaganda;

Mindful of the need to ensure a proper balance between freedom of expression and an effective fight against acts of a racist and xenophobic nature;

Recognising that this Protocol is not intended to affect established principles relating to freedom of expression in national legal systems;

Taking into account the relevant international legal instruments in this field, and in particular the Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocol No. 12 concerning the general prohibition of discrimination, the existing Council of Europe conventions on cooperation in the penal field, in particular the Convention on Cybercrime, the United Nations International Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965, the European Union Joint Action of 15 July 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning action to combat racism and xenophobia;

Welcoming the recent developments which further advance international understanding and cooperation in combating cybercrime and racism and xenophobia;

Having regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10-11 October 1997) to seek common responses to the developments of the new technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

CHAPTER I
COMMON PROVISIONS

Article 1
Purpose

The purpose of this Protocol is to supplement, as between the Parties to the Protocol, the provisions of the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001 (hereinafter referred to as "the Convention"), as regards the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Article 2
Definition

1. For the purposes of this Protocol, "racist and xenophobic material" means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.
2. The terms and expressions used in this Protocol shall be interpreted in the same manner as they are interpreted under the Convention.

CHAPTER II
MEASURES TO BE TAKEN AT NATIONAL LEVEL

Article 3
Dissemination of racist and xenophobic material through computer systems

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.
2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.
3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.

Article 4
Racist and xenophobic motivated threat

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason

that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

Article 5
Racist and xenophobic motivated insult

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.
2. A Party may either:
   a. require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or
   b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 6
Denial, gross minimisation, approval or justification of genocide or crimes against humanity

1. Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right: distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 April 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.
2. A Party may either
   a. require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise
   b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 7
Aiding and abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, aiding or abetting the commission of any of the offences established in accordance with this Protocol, with intent that such offence be committed.

CHAPTER III
RELATIONS BETWEEN THE CONVENTION AND THIS PROTOCOL

Article 8
Relations between the Convention and this Protocol

1. Articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Convention shall apply, *mutatis mutandis*, to this Protocol.
2. The Parties shall extend the scope of application of the measures defined in Articles 14 to 21 and Articles 23 to 35 of the Convention to Articles 2 to 7 of this Protocol.

CHAPTER IV
FINAL PROVISIONS

Article 9
Expression of consent to be bound

1. This Protocol shall be open for signature by the States which have signed the Convention, which may express their consent to be bound by either:
   a. signature without reservation as to ratification, acceptance or approval; or

b. signature subject to ratification, acceptance or approval, followed by ratification, acceptance or approval.

2. A State may not sign this Protocol without reservation as to ratification, acceptance or approval, or deposit an instrument of ratification, acceptance or approval, unless it has already deposited or simultaneously deposits an instrument of ratification, acceptance or approval of the Convention.

3. The instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

Article 10
Entry into force

1. This Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States have expressed their consent to be bound by the Protocol, in accordance with the provisions of Article 9.

2. In respect of any State which subsequently expresses its consent to be bound by it, the Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date of its signature without reservation as to ratification, acceptance or approval or deposit of its instrument of ratification, acceptance or approval.

Article 11
Accession

1. After the entry into force of this Protocol, any State which has acceded to the Convention may also accede to the Protocol.

2. Accession shall be effected by the deposit with the Secretary General of the Council of Europe of an instrument of accession which shall take effect on the first day of the month following the expiration of a period of three months after the date of its deposit.

Article 12
Reservations and declarations

1. Reservations and declarations made by a Party to a provision of the Convention shall be applicable also to this Protocol, unless that Party declares otherwise at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession.

2. By a written notification addressed to the Secretary General of the Council of Europe, any Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Articles 3, 5 and 6 of this Protocol. At the same time, a Party may avail itself, with respect to the provisions of this Protocol, of the reservation(s) provided for in Article 22, paragraph 2 and Article 41, paragraph 1, of the Convention, irrespective of the implementation made by that Party under the Convention. No other reservations may be made.

3. By a written notification addressed to the Secretary General of the Council of Europe, any state may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for in Article 5, paragraph 2.a and Article 6, paragraph 2.a of this Protocol.

Article 13
Status and withdrawal of reservations

1. A Party that has made a reservation in accordance with Article 12 above shall withdraw such reservation, in whole or in part, as soon as circumstances so permit. Such withdrawal shall take effect on the date of receipt of a notification addressed to the Secretary General of the Council of Europe. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2. The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations in accordance with Article 12 as to the prospects for withdrawing such reservation(s).

Article 14
Territorial application

1. Any Party may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Protocol shall apply.

2. Any Party may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Protocol to any other territory specified in the declaration. In respect of such territory, the Protocol shall enter into force on the first day of

the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 15
Denunciation

1. Any Party may, at any time, denounce this Protocol by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 16
Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Protocol as well as any State which has acceded to, or has been invited to accede to, this Protocol of:

a. any signature;

b. the deposit of any instrument of ratification, acceptance, approval or accession;

c. any date of entry into force of this Protocol in accordance with Articles 9, 10 and 11;

d. any other act, notification or communication relating to this Protocol.

In witness whereof the undersigned, being duly authorised thereto, have signed this Protocol.

EUROPEAN UNION

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection

of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12) Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

(13) Whereas the acitivities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the acitivities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15) Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17) Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association;

(33) Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

(34) Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35) Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals

with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities

(38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(39) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational meas-

ures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48) Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49) Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50) Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51) Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52) Whereas, in this context, ex post facto verification by the competent authorities must in general be considered a sufficient measure;

(53) Whereas, however, certain processing operation are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

(54) Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private of public law, who fails to comply with the national measures taken under this Directive;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of

personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction they fall;

(64) Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure as laid down in Council Decision 87/373/EEC (1);

(67) Whereas an agreement on a modus vivendi between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994;

(68) Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in

order to facilitate their cost-effective implementation, a further period expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas, where data contained in such filing systems are manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the way of a Member State's regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I
GENERAL PROVISIONS

Article 1
Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2
Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3
Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

   - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
   - by a natural person in the course of a purely personal or household activity.

Article 4
National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

   (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

   (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

   (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II
GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

SECTION I
PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

   (a) processed fairly and lawfully;

   (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

   (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

   (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

   (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II
CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III
SPECIAL CATEGORIES OF PROCESSING

Article 8
The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

   (a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

   (b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

   (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

   (d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

   (e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept

only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9
Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV
INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10
Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11
Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

   (a) the identity of the controller and of his representative, if any;

   (b) the purposes of the processing;

   (c) any further information such as

   - the categories of data concerned,
   - the recipients or categories of recipients,
   - the existence of the right of access to and the right to rectify the data concerning him

   in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V
THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12
Right of access

Member States shall guarantee every data subject

the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI
EXEMPTIONS AND RESTRICTIONS

Article 13
Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

   (a) national security;

   (b) defence;

   (c) public security;

   (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

   (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

   (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

   (g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

SECTION VII
THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14
The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15
Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which

produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

   (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

   (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

SECTION VIII
CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16
Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17
Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

   Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

   - the processor shall act only on instructions from the controller,
   - the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

SECTION IX
NOTIFICATION

Article 18
Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

   - where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or
   - where the controller, in compliance with the national law which governs him, ap-

points a personal data protection official, responsible in particular:

- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19
Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

   (a) the name and address of the controller and of his representative, if any;

   (b) the purpose or purposes of the processing;

   (c) a description of the category or categories of data subject and of the data or categories of data relating to them;

   (d) the recipients or categories of recipient to whom the data might be disclosed;

   (e) proposed transfers of data to third countries;

   (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20
Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21
Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

   The register shall contain at least the information listed in Article 19 (1) (a) to (e).

The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.

   Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

CHAPTER III
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.

CHAPTER IV
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25
Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

   Member States shall take the measures necessary to comply with the Commission's decision.

Article 26
Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of

personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

   If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2). Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER V
CODES OF CONDUCT

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

   Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI
SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28
Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

   These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

   - investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
   - effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
   - the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

   Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

   Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

   The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29
Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.

   It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the

Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Article 30

1. The Working Party shall:

   (a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

   (b) give the Commission an opinion on the level of protection in the Community and in third countries;

   (c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

   (d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VII
COMMUNITY IMPLEMENTING MEASURES

Article 31
The Committee

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.

   The opinion shall be delivered by the majority laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

   The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. It that event:

- the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,
- the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.

   When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

   By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

Article 34

This Directive is addressed to the Member States.

Done at Luxembourg, 24 October 1995.
For the European Parliament
The President K. HAENSCH
For the Council
The President L. ATIENZA SERNA

[1] OJ No C 277, 5. 11. 1990, p. 3 and OJ No C 311, 27. 11. 1992, p. 30.

[2] OJ No C 159, 17. 6. 1991, p 38.

[3] Opinion of the European Parliament of 11 March 1992 (OJ No C 94, 13. 4. 1992, p. 198), confirmed on 2 December 1993 (OJ No C 342, 20. 12. 1993, p. 30); Council common position of 20 February 1995 (OJ No C 93, 13. 4. 1995, p. 1) and Decision of the European Parliament of 15 June 1995 (OJ No C 166, 3. 7. 1995).

[4] OJ No L 197, 18. 7. 1987, p. 33.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof,

Having regard to the proposal from the Commission(1),

Having regard to the opinion of the Economic and Social Committee(2),

Having regard to the opinion of the Committee of the Regions(3),

Acting in accordance with the procedure laid down in Article 251 of the Treaty(4),

Whereas:

(1) On 16 April 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on a European Initiative in Electronic Commerce;

(2) On 8 October 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on ensuring security and trust in electronic communication - towards a European framework for digital signatures and encryption;

(3) On 1 December 1997 the Council invited the Commission to submit as soon as possible a proposal for a Directive of the European Parliament and of the Council on digital signatures;

(4) Electronic communication and commerce necessitate " electronic signatures" and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States may create a significant barrier to the use of electronic communications and electronic commerce; on the other hand, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies; legislation in the Member States should not hinder the free movement of goods and services in the internal market;

(5) The interoperability of electronic-signature products should be promoted; in accordance with Article 14 of the Treaty, the internal market comprises an area without internal frontiers in which the free movement of goods is ensured; essential requirements specific to electronic-signature products must be met in order to ensure free movement within the internal market and to build trust in electronic signatures, without prejudice to Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods(5) and Council Decision 94/942/CFSP of 19 December 1994 on the joint action adopted by the Council concerning the control of exports of dual-use goods(6);

(6) This Directive does not harmonise the provision of services with respect to the confidentiality of information where they are covered by national provisions concerned with public policy or public security;

(7) The internal market ensures the free movement of persons, as a result of which citizens and residents of the European Union increasingly need to deal with authorities in Member States other than the one in which they reside; the availability of electronic communication could be of great service in this respect;

(8) Rapid technological development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically;

(9) Electronic signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures;

(10) The internal market enables certification-service-providers to develop their cross-border activities with a view to increasing their competitiveness, and thus to offer consumers and businesses new opportunities to exchange information and trade electronically in a secure way, regardless of frontiers; in order to stimulate the Community-wide provision of certification services over open networks, certification-service-providers should be free to provide their services without prior authorisation; prior authorisation means not only any permission whereby the certification-service-provider concerned has to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect;

(11) Voluntary accreditation schemes aiming at an enhanced level of service-provision may offer certification-service-providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market; such schemes should encourage the development of best practice among certification-service-providers; certification-service-providers should be left free to adhere to and benefit from such accreditation schemes;

(12) Certification services can be offered either by a public entity or a legal or natural person, when it is established in accordance with the national law; whereas Member States should not prohibit certification-service-providers from operating outside voluntary accreditation schemes; it should be ensured that such accreditation schemes do not reduce competition for certification services;

(13) Member States may decide how they ensure the supervision of compliance with the provisions laid down in this Directive; this Directive does not preclude the establishment of private-sector-based supervision systems; this Directive does not oblige certification-service-providers to apply to be supervised under any applicable accreditation scheme;

(14) It is important to strike a balance between consumer and business needs;

(15) Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate; the functioning of the internal market requires the Commission and the Member States to act swiftly to enable the bodies charged with the conformity assessment of secure signature devices with Annex III to be designated; in order to meet market needs conformity assessment must be timely and efficient;

(16) This Directive contributes to the use and legal recognition of electronic signatures within the Community; a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; the legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognised;

(17) This Directive does not seek to harmonise national rules concerning contract law, particularly the formation and performance of contracts, or other formalities of a non-contractual nature concerning signatures; for this reason the provisions concerning the legal effect of electronic signatures should be without prejudice to requirements regarding form laid down in national law with regard to the conclusion of contracts or the rules determining where a contract is concluded;

(18) The storage and copying of signature-creation data could cause a threat to the legal validity of electronic signatures;

(19) Electronic signatures will be used in the public sector within national and Community administrations and in communications between such administrations and with citizens and economic operators, for example in the public procurement, taxation, social security, health and justice systems;

(20) Harmonised criteria relating to the legal effects of electronic signatures will preserve a coherent legal framework across the Community; national law lays down different requirements for the legal validity of hand-written signatures; whereas certificates can be used to confirm the identity of a person signing electronically; advanced electronic signatures based on qualified certificates aim at a higher level of security; advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device can be regarded as legally equivalent to hand-written signatures only if the requirements for hand-

written signatures are fulfilled;

(21) In order to contribute to the general acceptance of electronic authentication methods it has to be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States; the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorisation of the certification-service-provider involved; national law governs the legal spheres in which electronic documents and electronic signatures may be used; this Directive is without prejudice to the power of a national court to make a ruling regarding conformity with the requirements of this Directive and does not affect national rules regarding the unfettered judicial consideration of evidence;

(22) Certification-service-providers providing certification-services to the public are subject to national rules regarding liability;

(23) The development of international electronic commerce requires cross-border arrangements involving third countries; in order to ensure interoperability at a global level, agreements on multilateral rules with third countries on mutual recognition of certification services could be beneficial;

(24) In order to increase user confidence in electronic communication and electronic commerce, certification-service-providers must observe data protection legislation and individual privacy;

(25) Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Community or national law;

(26) The measures necessary for the implementation of this Directive are to be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission(7);

(27) Two years after its implementation the Commission will carry out a review of this Directive so as, inter alia, to ensure that the advance of technology or changes in the legal environment have not created barriers to achieving the aims stated in this Directive; it should examine the implications of associated technical areas and submit a report to the European Parliament and the Council on this subject;

(28) In accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty, the objective of creating a harmonised legal framework for the provision of electronic signatures and related services cannot be sufficiently achieved by the Member States and can therefore be better achieved by the Community; this Directive does not go beyond what is necessary to achieve that objective,

HAVE ADOPTED THIS DIRECTIVE:

Article 1
Scope

The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market.

It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents.

Article 2
Definitions

For the purpose of this Directive:

1. "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

2. "advanced electronic signature" means an electronic signature which meets the following requirements:

   (a) it is uniquely linked to the signatory;

   (b) it is capable of identifying the signatory;

   (c) it is created using means that the signatory can maintain under his sole control; and

   (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

3. "signatory" means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;

4. "signature-creation data" means unique data,

such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

5. "signature-creation device" means configured software or hardware used to implement the signature-creation data;

6. "secure-signature-creation device" means a signature-creation device which meets the requirements laid down in Annex III;

7. "signature-verification-data" means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;

8. "signature-verification device" means configured software or hardware used to implement the signature-verification-data;

9. "certificate" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;

10. "qualified certificate" means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II;

11. "certification-service-provider" means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;

12. "electronic-signature product" means hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;

13. "voluntary accreditation" means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

Article 3
Market access

1. Member States shall not make the provision of certification services subject to prior authorisation.

2. Without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification-service-providers for reasons which fall within the scope of this Directive.

3. Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public.

4. The conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States. The Commission shall, pursuant to the procedure laid down in Article 9, establish criteria for Member States to determine whether a body should be designated.

   A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognised by all Member States.

5. The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognised standards for electronic-signature products in the Official Journal of the European Communities. Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards.

6. Member States and the Commission shall work together to promote the development and use of signature-verification devices in the light of the recommendations for secure signature-verification laid down in Annex IV and in the interests of the consumer.

7. Member States may make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not con-

stitute an obstacle to cross-border services for citizens.

Article 4
Internal market principles

1. Each Member State shall apply the national provisions which it adopts pursuant to this Directive to certification-service-providers established on its territory and to the services which they provide. Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive.
2. Member States shall ensure that electronic-signature products which comply with this Directive are permitted to circulate freely in the internal market.

Article 5
Legal effects of electronic signatures

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:

   (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and

   (b) are admissible as evidence in legal proceedings.
2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

   - in electronic form, or
   - not based upon a qualified certificate, or
   - not based upon a qualified certificate issued by an accredited certification-service-provider, or
   - not created by a secure signature-creation device.

Article 6
Liability

1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:

   (a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;

   (b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;

   (c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;

   unless the certification-service-provider proves that he has not acted negligently.
2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.
3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate. provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.
4. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties.

   The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded.
5. The provisions of paragraphs 1 to 4 shall be without prejudice to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts(8).

Article 7
International aspects

1. Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if:

   (a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or

   (b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or

   (c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

2. In order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries, the Commission shall make proposals, where appropriate, to achieve the effective implementation of standards and international agreements applicable to certification services. In particular, and where necessary, it shall submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multilateral agreements with third countries and international organisations. The Council shall decide by qualified majority.

3. Whenever the Commission is informed of any difficulties encountered by Community undertakings with respect to market access in third countries, it may, if necessary, submit proposals to the Council for an appropriate mandate for the negotiation of comparable rights for Community undertakings in these third countries. The Council shall decide by qualified majority.

   Measures taken pursuant to this paragraph shall be without prejudice to the obligations of the Community and of the Member States under relevant international agreements.

Article 8
Data protection

1. Member States shall ensure that certification-service-providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on tile protection of individuals with regard to the processing of personal data and on the free movement of such data(9).

2. Member States shall ensure that a certification-service-provider which issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject.

3. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name.

Article 9
Committee

1. The Commission shall be assisted by an "Electronic-Signature Committee", hereinafter referred to as "the committee".

2. Where reference is made to this paragraph, Articles 4 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

   The period laid down in Article 4(3) of Decision 1999/468/EC shall be set at three months.

3. The Committee shall adopt its own rules of procedure.

Article 10
Tasks of the committee

The committee shall clarify the requirements laid down in the Annexes of this Directive, the criteria referred to in Article 3(4) and the generally recognised standards for electronic signature products established and published pursuant to Article 3(5), in accordance with the procedure laid down in Article 9(2).

Article 11
Notification

1. Member States shall notify to the Commission and the other Member States the following:

   (a) information on national voluntary accreditation schemes, including any additional requirements pursuant to Article 3(7);

   (b) the names and addresses of the national bodies responsible for accreditation and supervision as well as of the bodies referred to in Article 3(4);

   (c) the names and addresses of all accredited national certification service providers.

2. Any information supplied under paragraph 1 and changes in respect of that information shall be notified by the Member States as soon as possible.

Article 12
Review

1. The Commission shall review the operation of this Directive and report thereon to the European Parliament and to the Council by 19 July 2003 at the latest.

2. The review shall inter alia assess whether the scope of this Directive should be modified, taking account of technological, market and legal developments. The report shall in particular include an assessment, on the basis of experience gained, of aspects of harmonisation. The report shall be accompanied, where appropriate, by legislative proposals.

Article 13
Implementation

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 19 July 2001. They shall forthwith inform the Commission thereof.

   When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall communicate to the Commission the text of the main provisions of domestic law which they adopt in the field governed by this Directive.

Article 14
Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities

Article 15
Addressees

This Directive is addressed to the Member States.

Done at Brussels, 13 December 1999.
For the European Parliament
The President N. FONTAINE
For the Council
The President S. HASSI

[1] OJ C 325, 23.10.1998, p. 5.

[2] OJ C 40, 15.2.1999, p. 29.

[3] OJ C 93, 6.4.1999, p. 33.

[4] Opinion of the European Parliament of 13 January 1999 (OJ C 104, 14.4.1999, p. 49), Council Common Position of 28 June 1999 (OJ C 243, 27.8.1999, p. 33) and Decision of the European Parliament of 27 October 1999 (not yet published in the Official Journal). Council Decision of 30 November 1999.

[5] OJ L 367, 31.12.1994, p. 1. Regulation as amended by Regulation (EC) No 837/95 (OJ L 90, 21.4.1995, p. 1).

[6] OJ L 367, 31.12.1994, p. 8. Decision as last amended by Decision 99/193/CFSP (OJ L 73, 19.3.1999, p. 1).

[7] OJ L 184, 17.7.1999, p. 23.

[8] OJ L 95, 21.4.1993, p. 29.

[9] OJ L 281, 23.11.1995, p. 31.

ANNEX I

Requirements for qualified certificates

Qualified certificates must contain:

(a) an indication that the certificate is issued as a qualified certificate;

(b) the identification of the certification-service-provider and the State in which it is established;

(c) the name of the signatory or a pseudonym, which shall be identified as such;

(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

(e) signature-verification data which correspond to signature-creation data under the control of the signatory;

(f) an indication of the beginning and end of the period of validity of the certificate;

(g) the identity code of the certificate;

(h) the advanced electronic signature of the certification-service-provider issuing it;

(i) limitations on the scope of use of the certificate, if applicable; and

(j) limits on the value of transactions for which the certificate can be used, if applicable.

ANNEX II

Requirements for certification-service-providers issuing qualified certificates

Certification-service-providers must:

(a) demonstrate the reliability necessary for providing certification services;

(b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;

(c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;

(d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;

(e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature techology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;

(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

(h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

(i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

(j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;

(k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in redily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;

(l) use trustworthy systems to store certificates in a verifiable form so that:

- only authorised persons can make entries and changes,
- information can be checked for authenticity,
- certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
- any technical changes compromising these security requirements are apparent to the operator.

ANNEX III

Requirements for secure signature-creation devices

1. Secure signature-creation devices must, by appropriate technical and procedural means, en-

sure at the least that:

(a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;

(b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;

(c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

ANNEX IV

Recommendations for secure signature verification

During the signature-verification process it should be ensured with reasonable certainty that:

(a) the data used for verifying the signature correspond to the data displayed to the verifier;

(b) the signature is reliably verified and the result of that verification is correctly displayed;

(c) the verifier can, as necessary, reliably establish the contents of the signed data;

(d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;

(e) the result of verification and the signatory's identity are correctly displayed;

(f) the use of a pseudonym is clearly indicated; and

(g) any security-relevant changes can be detected.

Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime

SUMMARY

Europe's transition to an information society is being marked by profound developments in all aspects of human life: in work, education and leisure, in government, industry and trade. The new information and communication technologies are having a revolutionary and fundamental impact on our economies and societies. The success of the information society is important for Europe's growth, competitiveness and employment opportunities, and has far-reaching economic, social and legal implications.

The Commission launched the eEurope initiative in December 1999 in order to ensure that Europe can reap the benefits of the digital technologies and that the emerging information society is socially inclusive. In June 2000, The Feira European Council adopted a comprehensive eEurope Action Plan and called for its implementation before the end of 2002. The Action Plan highlights the importance of network security and the fight against cybercrime.

Information and communication infrastructures have become a critical part of our economies. Unfortunately, these infrastructures have their own vulnerabilities and offer new opportunities for criminal conduct. These criminal activities may take a large variety of forms and may cross many borders. Although, for a number of reasons, there are no reliable statistics, there is little doubt that these offences constitute a threat to industry investment and assets, and to safety and confidence in the information society. Some recent examples of denial

of service and virus attacks have been reported to have caused extensive financial damage.

There is scope for action both in terms of preventing criminal activity by enhancing the security of information infrastructures and by ensuring that the law enforcement authorities have the appropriate means to act, whilst fully respecting the fundamental rights of individuals.

The European Union has already taken a number of steps to fight harmful and illegal content on the Internet, to protect intellectual property and personal data, to promote electronic commerce and the use of electronic signatures and to enhance the security of transactions. In April 1998, the Commission presented to the Council the results of a study on computer-related crime (the so-called 'COMCRIME' study). In October 1999, the Tampere Summit of the European Council concluded that high-tech crime should be included in the efforts to agree on common definitions and sanctions. The European Parliament has also called for commonly acceptable definitions of computer-related offences and for effective approximation of legislation, in particular in substantive criminal law. The Council of the European Union has adopted a Common Position on the Council of Europe cybercrime convention negotiations and has adopted a number of initial elements as part of the Union's strategy against high-tech crime. Some EU Member States have also been at the forefront of relevant G8 activities.

This Communication discusses the need for and possible forms of a comprehensive policy initiative in the context of the broader Information Society and Freedom, Security and Justice objectives for improving the security of information infrastructures and combating cybercrime, in accordance with the commitment of the European Union to respect fundamental human rights.

In the short-term, the Commission believes that there is a clear need for an EU instrument to ensure that Members States have effective sanctions in place to combat child pornography on the Internet. The Commission will introduce later this year a proposal for a Framework Decision which, within the wider context of a package covering issues associated with the sexual exploitation of children and trafficking in human beings, will include provisions for the approximation of laws and sanctions.

In the longer-term, the Commission will bring forward legislative proposals to further approximate substantive criminal law in the area of high-tech crime. In accordance with the conclusions of the European Council in Tampere in October 1999, the Commission will also consider the options for mutual recognition of pre-trial orders associated with cybercrime investigations.

In parallel, the Commission intends to promote the creation of specialised computer-crime police units at the national level, where they do not already exist, support appropriate technical training for law enforcement and encourage European information security actions.

At the technical level and in line with the legal framework, the Commission will promote R&D to understand and reduce vulnerabilities and will stimulate the dissemination of know-how.

The Commission intends also to set up an EU Forum in which law enforcement agencies, Internet Service Providers, telecommunications operators, civil liberties organisations, consumer representatives, data protection authorities and other interested parties will be brought together with the aim of enhancing mutual understanding and co-operation at EU level. The Forum will seek to raise public awareness of the risks posed by criminals on the Internet, to promote best practice for security, to identify effective counter-crime tools and procedures to combat computer-related crime and to encourage further development of early warning and crisis management mechanisms.

TABLE OF CONTENTS

1. Opportunities and Threats in the Information Society

The increasing affordability and use of the Information Society Technologies (ISTs) and the globalisation of the economy are characteristics of our era. Further technological development and growth in use of open networks, such as the Internet, over the coming years will provide major new opportunities and will pose new challenges.

At the Lisbon Summit of March 2000, the European Council stressed the importance of the transition to a competitive, dynamic and knowledge-based economy, and invited the Council and the Commission to draw up an eEurope Action plan to make most of this opportunity.[1] This Action Plan, prepared by the Commission and the Council, adopted by the Feira Summit of the European Council in June 2000, includes actions to enhance network security and the establishment of a co-ordinated and coherent approach to cybercrime by the end of 2002.[2]

The information infrastructure has become a critical part of the backbone of our economies. Users should be able to rely on the availability of information services and have the confidence that their communications and data are safe from unauthorised access or modification. The take up of electronic commerce and the full realisation of Information Society depend on this.

The new digital and wireless technologies are already all pervasive. They give us the freedom to be mobile and yet always be connected, connected to a myriad of services built upon networks of networks. They give us the possibility to participate; to teach and to learn, to play together and to work together, to get involved in the political process. As societies though become increasingly reliant on these technologies, effective practical and legal means will have to be employed to help manage the associated risks.

Information Society Technologies (ISTs) can be and are being used for perpetrating and facilitating various criminal activities. In the hands of persons acting with bad faith, malice, or grave negligence, these technologies may become tools for activities that endanger or injure, the life, property or dignity of individuals or damage the public interest.

The classical security approach called for strict organisational, geographic and structural compartmentalisation of information according to sensitivity and category. This is no longer really feasible in this digital world since information processing is distributed, services follow mobile users and interoperability of systems is a prerequisite. Innovative solutions relying on emerging technologies are replacing traditional security approaches. These solutions involve the use of encryption and digital signatures, new access control and authentication tools and software filters of all kinds[3]. Ensuring secure and reliable information infrastructures not only requires a range of technologies but also their correct deployment and effective use. Some of these technologies already exist but often users are either not aware of their existence, of the ways to use them, or of the reasons why they may even be necessary.

1.1. NATIONAL AND INTERNATIONAL RESPONSES

Computer-related crimes are committed across cyber space and do not stop at the conventional state-borders. They can, in principle, be perpetrated from anywhere and against any computer user in the world. It has been generally recognised that effective action to combat computer-related crime is

1 Presidency Conclusions of the Lisbon European Council of 23 and 24 March 2000, available at http://ue.eu.int/en/Info/eurocouncil/index.htm.
2 http://europa.eu.int/comm/information_society/eeurope/actionplan/index_en.htm.
3 Information flows are filtered and controlled at all levels; from the firewall that looks at data packets, through the filter that looks for malicious software, the e-mail filter that discretely eliminates spam, to the browser filter that prevents access to harmful material.

necessary at both national and international level.[4]

On the national level, comprehensive and internationally oriented answers to the new challenges of network security and computer crime are often still missing. In most countries, reactions to computer crime focus on national law (especially criminal law), neglecting alternative preventive measures.

Despite the efforts of international and supranational organisations, the various national laws worldwide show remarkable differences, especially with respect to the criminal law provisions on hacking, trade secret protection and illegal content. Considerable differences also exist with respect to the coercive powers of investigative agencies (especially with respect to encrypted data and investigations in international networks), the range of jurisdiction in criminal matters, and with respect to the liability of intermediary service providers on the one hand and content providers on the other hand. Directive 2000/31/EC[5] on electronic commerce amends this as regards the liability of intermediary service providers on certain intermediary activities. The Directive also prohibits Member States from imposing such intermediary service providers a general obligation to monitor the information which they transmit or store.

On the international and supranational levels, the need to effectively combat computer-related crime has been broadly recognised and various organisations have been co-ordinating or attempting to harmonise relevant activities. The G8 Justice and Home Affairs Ministers adopted a set of principles and a 10-point action plan in December 1997, which was endorsed by the G8 Birmingham summit in May 1998 and is currently being implemented.[6] The Council of Europe (C.o.E.) started preparing an international convention on cyber-crime in February 1997 and is expected to complete this task in 2001.[7] Combating cybercrime is also on the agenda in bilateral discussions the European Commission has with some governments (apart from the EU). A Joint EC/US Task Force on Critical Infrastructure Protection has been established.[8]

The UN and OECD have also been active in this area, and it is being discussed in international fora such as the Global Business Dialogue and the Trans-Atlantic Business Dialogue.[9]

At the European Union level, until recently, legislative action has mainly taken the form of measures in the fields of copyright, the protection of the fundamental right to privacy and data protection, conditional access services, electronic commerce, electronic signatures and in particular the liberalisation of trade in encryption products, which are indirectly related to computer crime.

A number of important non-legislative measures have also been taken in the last 3-4 years. These include the Action Plan against illegal and harmful content on the Internet which co-finances awareness actions, experiments in rating and filtering of content and hot-lines, and initiatives concerning the protection of minors and human dignity in the information society, child pornography and interception of communications for law-enforcement purpos-

4 See, e.g., the e-Europe Action Plan at http://europa.eu.int/comm/information_society/eeurope/actionplan/index_en.htm, and statements of European Commissioner Antõnio Vitorino at http://europa.eu.int/comm/commissioners/vitorino/speeches/2000/septembre/2000-19-09-en_brussels.pdf, and French Prime Minister Lionel Jospin at http://www.france.diplomatie.fr/actual/evenements/cybercrim/jospin.gb.html.

5 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain aspects of Information Society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce").

6 The EU JHA Council on 19 March 1998 endorsed the 10 Principles to combat high-tech crime adopted by the G8 and invited the non-G8 Countries Member States of the EU to arrange for to join the network. Available on European Judicial Network website http://ue.eu.int/ejn/index.htm.

7 The Draft text is available on the web, in two languages, in French: http://conventions.coe.int/treaty/fr/projets/cybercrime.htm.

8 Under the auspices of the Joint Consultative Group of the EC/US Science and Technology Co-operation Agreement.

9 The United Nations produced a comprehensive "Manual on the prevention and control of computer-related crime," which has recently been updated. In 1983, the OECD undertook a study of the possibility of an international application and harmonisation of criminal laws to address the problem of computer crime or abuse. In 1986, it published "Computer-Related Crime: Analysis of Legal Policy," a report that surveyed the existing laws and proposals for reform in a number of Member States and recommended a minimum list of abuses that countries should consider prohibiting and penalising by criminal laws. Finally, in 1992, the OECD developed a set of guidelines for the security of information systems, which is intended to provide a foundation on which States and the private sector could construct a framework for the security of information systems.

es.[10] The EU has for a long time been supporting R&D Projects which aim at promoting security and trust in information infrastructures and electronic transactions and has recently increased the associated IST Programme budget allocations. Research and operational projects aimed at promoting specialised training of law enforcement personnel as well as co-operation between law enforcement and industry have also been supported in the framework of the Third Pillar Programmes such as STOP, FALCONE, OISIN and GROTIUS.[11]

The Action Plan to combat organised crime, adopted by the JHA Council in May 1997 and endorsed by the European Council of Amsterdam, included a request for a study on computer related crime to be prepared by the Commission by the end of year 1998. This study, the so-called 'COMCRIME study,' was presented by the Commission to the Council Multi-Disciplinary Working Group against organised crime in April 1998.[12] This Communication is partly a follow-up to the JHA Council request.

Before drafting this Communication, the Commission considered it appropriate to undertake informal consultations with representatives from Member States law enforcement and data protection supervisory authorities[13] and from the European industry (mostly ISPs and telecommunications operators).[14]

On the basis of the analysis and the recommendations made by the study, the conclusions drawn from the consultation process, the new possibilities provided for by the Treaty of Amsterdam and the work already accomplished in the EU, the G8 and the C.o.E., this Communication will examine various options for further action by the EU against computer-related crime. On the European Union level the chosen solutions should not lead to any impediment for and fragmentation of the Internal Market, nor to measures which undermine the protection of fundamental rights.[15]

2. SECURITY OF INFORMATION INFRASTRUCTURES

In the information society, user-controlled global networks are gradually replacing the older generation of national communication networks. One of the reasons for the success of the Internet is that it has given users access to the very newest technologies. Moore's Law[16] predicts that computing power doubles every 18 months. Communications technology however is developing at an even faster pace.[17] One result of this is that the volume of data carried over the Internet has been doubling in periods of less than a year.

The classical telephone networks were constructed and operated by national organisations. Its users had little choice of services and no control over the environment. The first data networks that were developed were built on the same philosophy of a centrally controlled environment. Security within these environments reflected this.

10 Council Recommendation 98/560/EC of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity; Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services; COM(96) 483, October 1996, http://europa.eu.int/en/record/green/gp9610/protec.htm; Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions -Illegal and harmful content on the Internet (COM(96) 487 final); Resolution on the Commission communication on illegal and harmful content on the Internet (COM(96)487 - C4-0592/96); Council Resolution of 17 January 1995 on the lawful interception of telecommunications (OJ C 329, 04.11.1996, pp. 1- 6).

11 http://europa.eu.int/comm/justice_home/jai/prog_en.htm.

12 "Legal Aspects of Computer-related Crime in the Information Society - COMCRIME." The study was prepared by Prof. U. Sieber of the University of Würzburg under contract with the European Commission. The final report is available at: http://europa.eu.int/ISPO/legal/en/crime/crime.html.

13 At EU level, the data protection supervisory authorities constitute the Article 29 Data Protection Working Party, which is the independent EU advisory body on privacy and data protection, see art. 29 and 30 of Directive 95/46/EC.

14 Two meetings with law enforcement took place on 10.12.1999 and 1.3.2000. A meeting with Internet industry representatives took place on 13.3.2000. A meeting with a small number of personal data protection experts took place on 31.3.2000. A final meeting with all the above took place on 17.4.2000. Minutes of the meetings can be obtained by writing to: European Commission, Unit INFSO/A4, or to: European Commission, Unit JAI/B2, Wetstraat/Rue de la Loi 200, 1049 Brussels, Belgium.

15 EU Charter on Fundamental Rights (http://europa.eu.int/comm/justice_home/unit/charte_en.htm), Article 6 of the TEU and jurisprudence of the European Court of Justice.

16 The observation made in 1965 by Gordon Moore, co-founder of Intel, about the speed at which the density of transistors in integrated circuits was increasing. This density is now approximately doubling every 18 months and this has a direct impact on the price and performance of computer chips. Many experts expect this to hold for at least another decade.

17 The latest technology makes it possible for a single optical fibre cable to simultaneously carry the equivalent of 100 million voice calls.

The Internet and other new networks are very different, and security needs to be handled accordingly. Intelligence and control in these networks is mostly at the periphery, where the users and services are. The core of the network is simple and efficient, and essentially dedicated to the task of transmitting data. There is limited checking or control of content. It is only at the final destination where the bits become the sound of a voice, the image of an x-ray or the confirmation of a bank transaction. Security is therefore to an important extent a responsibility of the users, as only they can appreciate the value of the bits being sent or received, and can determine the level of protection needed.

The user environment is therefore a key part of the information infrastructure. Security techniques have to be implemented there with the permission and participation of the user and according to his/her needs. This is particularly important when one considers the increasing range of activities that people are carrying out from the same terminal. They work and play, they watch television and authorise bank transfers, all from the same device.

Several security technologies are available and new technologies are being developed. The advantages of open source development in terms of security are becoming clearer. Much work has been done on formal methods and on security evaluation criteria. The use of encryption technologies and electronic signatures are becoming indispensable, particularly with the growth in wireless access. An increasing variety of authentication mechanisms is required to meet our different needs in the environments in which we interact. In some environments, we may need or wish to remain anonymous. In others, we may need to be able to prove a certain characteristic while not revealing our identity, such as being an adult or being an employee or a client of a particular company. In yet other situations, it may be necessary to give proof or our identity. Also software filters are becoming ever more sophisticated, and enable us to protect ourselves or those in our care from data we do not want, such as undesirable content, spam mail, malicious software and other forms of attack. The implementation and management of such security requirements within the Internet and new networks also involve considerable expense to industry and users. Therefore it is important to encourage innovation and commercial use of security technology and services.

Naturally, also the shared infrastructure of communication links and name-servers has its security aspects. Data transmission depends on the physical links whereby data is routed from one computer to another. These links have to be put in place and protected in such a way that transmission remains possible in spite of accidents, attacks and an ever increasing volume of traffic. Communication also depends on critical services such as those provided by the name servers, and in particular on the small number of root name servers, that provide the needed addresses. Each of these components will also need appropriate protection, which will vary according to the part of the name space and the user base that is being served.

Driven by the objective of bringing more flexibility and responsiveness to people's needs, information infrastructure technologies have become increasingly complex with often insufficient design effort devoted to security. In addition, this complexity involves more and more sophisticated and interconnected software programmes, which sometimes include weaknesses, security holes, that may easily be exploited for attacks. As cyberspace gets more and more complex and its components more and more sophisticated, new and unforeseen vulnerabilities may emerge.

Several technological mechanisms already exist and new ones are being developed to improve security in cyber-space. The response includes measures:

- To secure critical elements of the infrastructure through the deployment of public-key infrastructures (PKI), the development of secure protocols, etc.
- To secure private and public environments through the development of quality software, firewalls, anti-virus programs, electronic rights management systems, encryption, etc.
- To secure authentication of authorised users, use of smart cards, biometric identification, electronic signatures, role-based technologies, etc.

This calls for an increased effort to develop security technologies, involving co-operation in order to achieve a necessary interoperability between solutions through agreements on international standards.

It is important also that any future conceptual framework for security be an integral part of the overall architecture, addressing threats and vulnerabilities from the outset of the design process. This contrasts with traditional add-on approaches, which have necessarily attempted to plug the holes exploited by an increasingly sophisticated criminal community.

The EU Information Society Technologies (IST) Programme,[18] in particular work relating to information-, and network security, and other confidence-building technologies,[19] provides a framework to develop capability and technologies to understand and tackle emerging challenges related to computer crime. These technologies include technical tools to protect against infringement of the fundamental rights to privacy and personal data and other personal rights and to fight computer crime. In addition, in the context of the IST Programme, a dependability initiative has been launched. This initiative will contribute towards trust and confidence in highly inter-linked information infrastructures and in tightly networked embedded systems by promoting dependability awareness and dependability enabling technologies. An integral part of this initiative is international co-operation. The IST Programme has developed working relationships with DARPA and NSF and has established, in collaboration with the US Department of State, a Joint EC/US Task Force on Critical Infrastructure Protection.[20]

Finally, the implementation of security obligations following in particular from the EU Data Protection Directives[21] contributes to enhancing security of the networks and of data processing.

3. COMPUTER-RELATED CRIME

Modern information and communications systems make it possible to perform illegal activities from anywhere to anywhere in the world at any time. There are no reliable statistics available on the full scale of the computer-related crime phenomenon. The number of intrusions detected and reported up to now, probably under-represent the scope of the problem. Because of limited awareness and experience of system administrators and users, many intrusions are not detected. In addition, many companies are not willing to report cases of computer abuse, to avoid bad publicity and exposure to future attacks. Many police forces do not yet keep statistics on the use of computers and communication systems involved in these and other crimes. However, the number of illegal activities can be expected to grow as computer and network use increases. There is a clear need to gather reliable evidence on the significance of computer-related crime.

In this Communication, computer-related crime is addressed in the broadest sense, as any crime that in some way or other involves the use of information technology. However, different views exist on what constitutes "computer-related crime." The terms "computer crime," "computer-related crime," "high-tech crime" and "cybercrime" are often used interchangeably. A difference can be made between computer specific crimes and traditional crimes performed with the aid of computer technology. A topical example of this can be found in the realm of Customs where the Internet proves to be an instrument for committing typical crimes against Customs Law, such as smuggling, counterfeit, etc. Whereas the computer-specific crimes require updates of the definitions of crimes in national criminal codes, the traditional crimes performed with the aid of computers call for improved co-operation and procedural measures.

Yet all of them benefit from the availability of information and communication networks which are borderless and from the circulation of data which is intangible and extremely volatile. These characteristics call for a review of existing measures to address illegal activities performed on or using these networks and systems.

Many countries have passed legislation to address computer-related crime. In European Union Member States, a number of legal instruments have been issued. Other than a Council Decision on child pornography on the Internet, there are no EU legal instruments so far directly addressing computer-related crime, but there are a number of indirectly relevant legal instruments.

The main issues addressed by legislation in relation to computer specific crimes at EU or Member State level are:

Privacy Offences: Various countries have introduced criminal law addressing illegal collection, storage, modification, disclosure or dissemination of personal data. In the European Union, two Directives have been adopted that approximate the national laws on the protection of privacy with regard to

18 The IST Programme is managed by the European Commission. It is part of the 5th Framework Programme, which runs from 1998 to 2002. More information is available at http://www.cordis.lu/ist.

19 In Key Action 2 - New Methods of Work and Electronic Commerce.

20 Under the auspices of the Joint Consultative Group of the EC/US Science and Technology Co-operation Agreement.

21 See Article 4 of Directive 97/66/EC (including also an obligation to inform about remaining security risks) and Article 17 of Directive 95/46/EC.

the processing of personal data.[22] Article 24 of the Directive 95/46/EC clearly obliges Member States to adopt all suitable measures to ensure the full implementation of the provisions of the Directive, including sanctions to be imposed in case of infringements of the provisions of national laws. The fundamental rights to privacy and data protection are furthermore included in the Charter of Fundamental Rights of the European Union.

Content-related offences: The dissemination, especially via the Internet, of pornography, in particular child pornography, racist statements and information inciting violence raises the question as to what extent these acts could be confronted with the help of criminal law. The Commission has supported the view that what is illegal off-line should also be illegal on-line. The author or the content provider[23] may be liable under criminal law. A Council Decision has been adopted to combat child pornography on the Internet.[24]

The liability of the intermediary service providers, whose networks or servers are used for the transmission or storage of third-party information, has been addressed by the Directive on electronic commerce.

Economic crimes, unauthorised access and sabotage: Many countries have passed laws that address computer-specific economic crime and define new offences related to unauthorised access to computer systems (e.g., hacking, computer sabotage and distribution of viruses, computer espionage, computer forgery, and computer fraud[25]) and new forms of committing offences (e.g., computer manipulations instead of deceiving a human). The object of the crime is often intangible, e.g., money in bank deposits or computer programmes. At present, there are no EU instruments regarding such types of illegal activity. Concerning prevention, the recently adopted revised dual-use goods regulation contributed significantly to liberalise the availability of encryption products.

Intellectual Property Offences: Two Directives have been adopted, on the legal protection of computer programs and of databases,[26] relating directly to the Information Society and providing for sanctions. A Common Position on a proposal for a Directive on copyright and related rights in the Information Society has been adopted by the Council . This is expected to be adopted early 2001.[27] The violation of copyright and related rights as well as the circumvention of technological measures designed to protect these rights are to be sanctioned. As regards counterfeiting and piracy, the Commission will present, before the end of 2000, a Communication taking stock of the consultation process initiated with its 1998 Green Paper and announcing a relevant action plan. As the Internet becomes more and more important commercially, we are beginning to see new disputes around domain names related to cybersquatting, warehousing and reverse hijacking, and, naturally, there are also calls for rules and procedures to help deal with these problems.[28]

Enforcement of taxation obligations also needs to be addressed. In the case of commercial transactions where the recipient of on-line supply of an electronic service is located in the EU, this will in most cases give rise to tax obligations in the jurisdiction where consumption of such a service

22 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. Art. 24 of Directive 95/46/EC obliges Member States to lay down sanctions to be imposed in case of infringement of data protection provisions.

23 The content provider should not be confused with the service provider.

24 Council Decision of 29 May 2000 to combat child pornography on the Internet (OJ L 138, 9.6.2000, p.1).

25 The media has given much attention to the recent "distributed Denial of Service" attacks on large web-sites and the distribution of the so-called LoveBug virus. This however should be kept in perspective. Denial of service attacks, either deliberate or accidental, and e-mail related viruses have been around for many years. The Morris worm and the IBM Xmas-tree email were earlier examples. There exist products and procedures to help deal with these. There is also a great deal of good co-operation within the Internet community to limit the damage from such incidents as they happen. There is similar co-operation to limit spamming abuses.

26 Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs (OJ L 122 , 17.5.1991, pp. 42 - 46). Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (OJ L 77 , 27.3.1996, pp. 20 - 28).

27 Common Position adopted by the Council with a view to the adoption of a Directive of theEuropean Parliament and of the Council on harmonization of certain aspects of copyright and related rights in the Information Society (CS/2000/9512).

28 Communication from the Commission to the Council and the European Parliament, The Organisation and Management of the Internet; International and European Policy Issues 1998 - 2000, April 2000, COM(2000) 202.

is deemed to take place.[29] Failure to comply with tax obligations exposes an operator to civil (and in some cases criminal) sanctions which may include seizure of bank accounts or other assets. Although voluntary compliance is always the preferred option, such obligations must ultimately be enforceable.

Co-operation between tax administrations is a key element in achieving this objective. Giving the possibility to some people to protect their lawful transactions will also give the same means to criminals to protect their unlawful transactions. The tools that give us secure e-commerce can also be used to support drug trafficking. Priorities will need to be identified and choices will need to be made.

Protecting the victims of computer-related crime also needs to cover issues of liability, redress and compensation which arise when computer-related crimes do occur. Confidence depends not only on appropriate technology being used, but also on the accompanying legal and economic guarantees. These questions will need to be examined across the range of computer-related crimes.

There is a need for effective substantive and procedural law instruments approximated at global, or at least at European level, to protect the victims of computer-related crime and to bring the perpetrators to justice. At the same time, personal communications, privacy and data protection, access to and dissemination of information, are fundamental rights in modern democracies. This is why the availability and use of effective prevention measures are desirable so to reduce the need to apply enforcement measures. Any legislative measures that might be necessary to tackle computer-related crime need to strike the right balance between these important interests.

4. SUBSTANTIVE LAW ISSUES

Approximation of substantive law in the area of high tech crime will ensure a minimum level of protection for victims of cybercrime (for example, victims of child pornography), will help to meet the requirement that an activity must be an offence in both countries before mutual legal assistance can be provided to assist a criminal investigation (the dual criminality requirement), and will provide greater clarity for industry (for example, on what constitutes illegal content).

In fact, an EU legislative instrument approximating substantive criminal law in the field of computer-related crime has been on the EU agenda following the Tampere Summit of the European Council in October 1999.[30] The Summit included high-tech crime in a limited list of areas where efforts should be made to agree on common definitions, incriminations and sanctions. This is included in Recommendation 7 of the European Union strategy for the new Millennium on the prevention and control of organised crime adopted by the JHA Council in March 2000.[31] It is also part of the Commission Work Programme for the Year 2000 and the Scoreboard for the establishment of an area of Freedom, Security and Justice, produced by the Commission and adopted by the Justice and Home Affairs Council on 27 March 2000.[32]

The Commission has followed the work of the Council of Europe on the Cybercrime Convention. Four categories of criminal offences are listed in the current draft C.o.E. Cybercrime Convention: 1) Offences against the confidentiality, integrity and availability of computer data and systems; 2) Computer-related offences; 3) Content-related offences; 4) Offences related to infringements of copyright and related rights.

EU approximation could go further than the C.o.E. Convention, which will represent a minimum of international approximation. It could be operational within a shorter period of time than the entry into force of the C.o.E. Convention.[33] It would bring computer crime within the realms of EU law and introduce EU enforcement mechanisms.

The Commission attaches great importance to ensuring that the European Union is able to take effective action in particular against child pornography on the Internet. The Commission welcomes the Council Decision on combating child pornography on the Internet, but shares the view of the European Parliament that further action is required to ap-

29 The Commission has proposed a series of amendments to the EU VAT system aimed at clarifying the jurisdiction of tax liability (COM (2000) 349 - Proposal for a Council Directive amending Directive 77/388/EEC as regards the Value Added tax Arrangements applicable to certain services supplied by electronic means) which is currently under consideration in the Council and the Parliament. In some circumstances, however, the liability to pay tax may fall on the supplier, even when the supplier has no physical presence in the taxing jurisdiction.

30 http://db.consilium.eu.int/en/Info/eurocouncil/index.htm.

31 The Prevention and control of organised crime: A European Union strategy for the beginning of the new Millennium (OJ 2000 C124, 3.5.2000).

32 http://europa.eu.int/comm/dgs/justice_home/index_en.htm.

33 Entry into force of the C.o.E. Convention will only take place after ratification.

proximate national laws. The Commission intends to introduce later this year a proposal for a Council Framework Decision that will include provisions for the approximation of laws and sanctions on child pornography on the Internet.[34]

In accordance with the Tampere conclusions, the Commission will bring forward a legislative proposal under Title VI of the TEU to approximate high tech crime offences. This will build on the progress made at the Council of Europe, and will address in particular the need to approximate legislation relating to hacking and denial of service attacks. The proposal will include standard definitions for the European Union in this area. This could also go further than the draft Council of Europe Convention by ensuring that serious cases of hacking and denial of service attacks are punishable by a minimum penalty in all Member States.

Furthermore, the Commission will examine the scope for action against racism and xenophobia on the Internet with a view to bringing forward a proposal for a Council Framework Decision under Title VI of the TEU covering both off-line and on-line racist and xenophobic activity. This will take account of the forthcoming evaluation of the implementation by Member States of the Joint Action of 15 July 1996 concerning action to combat racism and xenophobia.[35] The Joint Action was a first step towards approximation of criminal offences relating to racism and xenophobia, but there is a need for further approximation within the European Union. The importance and sensitivity of this issue has been highlighted by the decision of a French court on 20 November 2000 requiring Yahoo to block French users from accessing sites selling Nazi memorabilia.[36]

Finally, the Commission will consider how to improve the effectiveness of efforts against the illicit drugs trade on the Internet, the importance of which is recognised in the European Union Drugs Strategy 2000-2004 endorsed at the European Council in Helsinki.[37]

5. PROCEDURAL LAW ISSUES

The very nature of computer-related criminal offences brings procedural issues to the forefront of national and international attention as different sovereignties, jurisdictions and laws come into play. More than in any other transnational crime, the speed, mobility and flexibility of computer crime challenge the existing rules of criminal procedural law.

Approximation of procedural law powers will improve the protection of victims by ensuring that law enforcement agencies have the powers they need to investigate offences on their own territory, and will ensure that they are able to respond quickly and effectively to requests from other countries for co-operation.

It is also important to ensure that measures taken on the basis of criminal law, which generally falls with the competence of Member States and Title VI of the TEU, are in accordance with Community law requirements. In particular, the Court of Justice has consistently held that such legislative provisions may not discriminate against persons to whom Community law gives the right to equal treatment or restrict the fundamental freedoms guaranteed by Community law.[38] Any new powers for law enforcement need to be assessed against Community law and their impact to privacy.

5.1. Interception of communications

In the European Union, there is a general principle of confidentiality of communications (and related traffic data). Interceptions are illegal unless they are authorised by law when necessary in specific cases for limited purposes. This follows from Article 8 of the European Convention of Human Rights, referred to in Article 6 of the TEU and more particularly from Directives 95/46/EC and 97/66/EC.

34 This initiative is part of a package of proposals which also covers wider issues associated with the sexual exploitation of children and trafficking in human beings, as announced in the Commission's Communication on trafficking in human beings of December 1998. The text of the proposal for a Council Framework decision is annexed to the Communication from the Commission to the Council and the European Parliament on combating trafficking in human beings an the sexual exploitation of children: two proposals for Framework Decisions which is being published in parallel with this Communication.

35 OJ, L185, 24.7.1996, p. 5-7. Also available on the European Judicial Network website http://ue.eu.int/ejn/index.htm.

36 Tribunal de Grande Instance de Paris, Ordonnance de Référé rendue le 20 November 2000, No. RG 00/05308.

37 EU Action Plan to Combat Drugs (2000 - 2004). COM(1999) 239 final, http://europa.eu.int/comm/justice_home/unit/drogue_en.htm.

38 Case C-274/96 Bickel & Franz (1998) ECR I-7637 para 17, Case C-186/87 Cowan (1989) ECR 195 para 19. In particular, the administrative measures or penalties must not go beyond what is strictly necessary, the control procedures must not be conceived in such a way as to restrict the freedom required by the Treaty and they must not be accompanies by a penalty which is so disproportionate to the gravity of infringement that it becomes an obstacle to the exercise of that freedom (Case C-203/80 Casati (1981) ECR 2595 para 27).

All Member States have a legal framework in place to allow law enforcement to obtain judicial orders (or, in the case of two Member States, a warrant personally authorised by a senior Minister) for the interception of communications on the public telecommunications network.[39] This legislation, which has to be in line with Community law to the extent that it applies, contains safeguards protecting individuals' fundamental right to privacy, such as limiting the use of interception to investigations of serious crimes, requiring that interception in individual investigations should be necessary and proportionate, or ensuring that the individual is informed about the interception as soon as it will no longer hamper the investigation. In many Member States, interception legislation contains obligations for (public service) telecommunications operators to provide for interception capabilities. A 1995 Council Resolution was aimed at co-ordinating interception requirements.[40]

Traditional network operators, in particular those offering voice services, have in the past established working relations with law enforcement to facilitate lawful interception of communications. Telecommunications liberalisation and the explosion of Internet use have attracted many entrants to the marketplace, who have been confronted afresh with interception requirements. Questions on regulations, technical feasibility, allocation of costs and commercial impact will need to be discussed in government-industry dialogues together with all other parties concerned including data protection supervisory authorities.

New technologies make it essential that Member States work together if they are to maintain their capabilities for lawful interception of communications. Where Member States introduce new technical interception requirements on telecommunications operators and Internet service providers, the Commission believes these standards should be co-ordinated internationally to prevent distortion of the Single Market, to minimise the costs for industry and to respect privacy and data protection requirements. The standards should be public and open where possible and should not introduce weaknesses into the communications infrastructure.

In the context of the EU Convention on Mutual Assistance in Criminal Matters,[41] an approach has been agreed to facilitate co-operation on legal interception.[42] The Convention contains provisions on the interception of satellite telephone communication,[43] and on interception of communications of a person on the territory of another Member State.[44] The Commission believes that the interception rules in the Mutual Legal Assistance Convention constitute the maximum possible at the current stage. The text of the Convention is technology neutral; it will have to be tested how it will work in practice before any improvements can be considered. The Commission will review its implementation with Member States, industry, users and data protection supervisory authorities to ensure that relevant initiatives are effective, transparent and well balanced.

Abusive, indiscriminate use of interception capa-

39 Two Member States do not allow intercepted communications as evidence in criminal proceedings.

40 Council Resolution of 17 January 1995 on the lawful interception of telecommunications (OJ C 329, 4.11.1996, pp. 1- 6). The Annex contains a list of law-enforcement interception requirements that Member States were requested to take into account in the definition and implementation of relevant national policies and measures. In 1998, the Austrian Presidency proposed an EU Council Resolution to extend the scope of the 1995 Resolution to cover new technologies, including Internet and satellite communications. This has been the subject of debate in two European Parliament Committees, the Committee on Civil Liberties and Internal Affairs and the Committee on Legal Affairs and Citizens' Rights, which reached different conclusions. The former considered this resolution to be a clarification and update of the old one and thought it was acceptable. The latter was strongly critical, both on potential human rights infringements and on the costs to operators, rejecting the EU Council proposal and calling on the Commission to draw up a new proposal once the Treaty of Amsterdam had entered into force. The draft Council Resolution has not been actively considered by the Council or its working parties in recent months.

41 O J C 197 of 12.7.2000, p.1. The Convention was adopted 29 May 2000. The interception provisions in the Convention apply only to the Member States of the European Union and not to third countries.

42 The Convention provides for minimum safeguards concerning the protection of privacy and personal data.

43 The initial purpose of the negotiations was to provide an interception capability concerning persons using satellite telephones on the territory of the intercepting Member State. Technically, the critical point to intercept these communications is at the satellite ground station. It was therefore necessary to seek technical assistance from the Member State where the ground station was located. The Convention contains two options that address this issue: an expedited mutual legal assistance procedure which requires individual requests for assistance to the Member State with the satellite ground station, and a technical solution based on remote access to the satellite ground station from the intercepting Member State which does not require individual requests.

44 The Convention also provides for a legal framework for requests for interception of the communications of a person on the territory of another Member State (the requested Member State). In this case, the intercepting Member State and the requested Member State both need to obtain interception warrants under their domestic laws. Finally, the Convention establishes rules to cover situations where the intercepting Member State may have the possibility to intercept the communications of a person on the territory of another Member State without the need to seek technical assistance from that Member State.

bilities, particularly internationally, will raise human rights questions and will undermine citizens' trust in the Information Society. The Commission has seen with grave concern reports on alleged abuses of interception capabilities.[45]

5.2. Retention of traffic data

To investigate and prosecute crimes involving the use of the communications networks, including the Internet, law enforcement authorities frequently use traffic data when they are stored by service providers for billing purposes. As the price charged for a communication is becoming less and less dependent on distance and destination, and service providers move towards flat rate billing, there will no longer be any need to store traffic data for billing purposes. Law enforcement authorities fear that this will reduce potential material for criminal investigations and therefore advocate that service providers keep certain traffic data for at least a minimum period of time so that these data may be used for law enforcement purposes.[46]

In accordance with the EU personal Data Protection Directives, both the general purpose-limitation principles of Directive 95/46/EC and the more specific provisions of Directive 97/66/EC, traffic data must be erased or made anonymous immediately after the telecommunications service is provided, unless they are necessary for billing purposes. For flat rate or free-of-charge access to telecommunications services, service providers are in principle not allowed to preserve traffic data.

Under the EU Data Protection Directives, Member States may adopt legislative measures to restrict the scope of the obligation to erase traffic data when this constitutes a necessary measure for, amongst others, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the telecommunications system.[47]

However, any legislative measure at national level that may provide for the retention of traffic data for law enforcement purposes would need to fulfil certain conditions: the proposed measures need to be appropriate, necessary and proportionate, as required by Community law and international law, including Directive 97/66/EC and 95/46/EC, the European Convention for the Protection of Human Rights of 4 November 1950 and the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 28 January 1981. This is particularly relevant for measures that would involve the routine retention of data on a large part of the population.

Some Member States are taking legal initiatives requiring or allowing service providers to store certain categories of traffic data, not needed for billing purposes, after the provision of the service but which are considered useful for criminal investigations.

The scope and form of these initiatives varies considerably, but they are all based on the idea that more data should be available for law enforcement authorities than would be the case if service providers only process data which are strictly needed for the provision of the service. The Commission is examining these measures in the light of existing Community law.

The European Parliament is sensitive to privacy issues and generally has taken a stance in favour of strong protection of personal data. However, in discussions on combating child pornography on the Internet, the European Parliament has expressed an opinion favouring a general obligation to preserve traffic data for a period of three months.[48]

This illustrates the importance of the context in which a sensitive topic such as traffic data retention is discussed and the challenge facing policy makers seeking to strike appropriate balances.

The Commission considers that any solution on the complex issue of retention of traffic data should be well founded, proportionate and achieve a fair balance between the different interests at stake. Only an approach that brings together the expertise and capacities of government, industry, data protection supervisory authorities and users will succeed in meeting such goals. A consistent approach in all Member States on this complex issue would be

45 A long, extensively documented report by Mr Campbell (http://www.gn.apc.org/duncan/stoa_cover.htm) on an intelligence interception network called ECHELON was the subject of a European Parliament public hearing. The report argues that ECHELON was conceived for national security purposes but has also been used for industrial espionage. The European Parliament has set up a temporary Committee that will study the subject and will submit a report to the plenary within a year.

46 These would include criminal investigations in cases that are not related to computers or communications networks, but where the data may help to resolve the crime.

47 Art. 14 of Directive 97/66/EC and art 13 of Directive 95/46/EC.

48 Legislative resolution embodying Parliament's opinion on the draft Joint Action, adopted by the Council on the basis of Article K.3 of the Treaty on European Union, to combat child pornography on the Internet, Amendment 17 (OJ C 219,30.7.1999, pp. 68 ff., on p. 71).

highly desirable, to meet the objectives of both effectiveness and proportionality and to avoid the situation where both law enforcement and the Internet community would have to deal with a patchwork of diverse technical and legal environments.

There are quite different important concerns to be taken into account. On one hand, data protection supervisory authorities have considered that the most effective means to reduce unacceptable risks to privacy while recognising the needs for effective law enforcement is that traffic data should in principle not be kept only for law enforcement purposes.[49] On the other hand, law enforcement authorities have stated that they consider the retention of a minimum amount of traffic data for a minimum period of time necessary to facilitate criminal investigations.

Industry has an interest to co-operate in the fight against crimes like hacking and computer-fraud, but should not be confronted with measures that are unreasonably costly. The economic impact of any measures should be carefully analysed and compared with the effectiveness of such a measure in the fight against cybercrime in order to avoid making the Internet more costly and less affordable for users. Adequate security of any retained traffic data would have to be ensured.

In any case, industry will have a key role to play in contributing, to the process of creating a safer Information Society. Users should have confidence in the safety of the Information Society and feel protected from crime and from infringements of their privacy.

The Commission fully supports and encourages a constructive dialogue between law enforcement, industry, data protection authorities and consumer organisations as well as other parties that might be concerned. Within the framework of the proposed EU Forum (see point 6.4 of this Communication), the Commission will urge all the parties concerned to discuss in-depth, as a matter of priority, the complex issue of retention of traffic data with a view to jointly finding appropriate, balanced and proportionate solutions fully respecting the fundamental rights to privacy and data protection.[50] On the basis of the outcome of this work, the Commission will be able to assess the need for any legislative or non-legislative actions at EU level.

5.3. Anonymous access and use

Law enforcement experts have expressed concern that anonymity may result in non-accountability and could seriously impede the possibility to catch certain criminals. Anonymous use of mobile telephony is possible in some countries through pre-pay cards (not in others). Anonymous access to and use of the Internet is offered by some service and access providers, including re-mailers and Internet cafés. A degree of anonymity is also facilitated by the system of dynamic Internet addressing, in which addresses are not allocated to users on a permanent basis but only for the duration of a given session.

In their discussions with the Commission, some representatives from industry have not been in favour of full anonymity, partly for their own security, anti-fraud and network integrity purposes. The London Internet Exchange has pointed to best practice guidelines they had issued which had proved useful in the UK.[51] However, other industry representatives and privacy experts have stated that without anonymity it is not possible to guarantee fundamental rights.

The Art. 29 Data Protection Working Party has issued a Recommendation on the subject of anonymous use of the Internet.[52] It considers the issue of anonymity on the Internet as being at the centre of a dilemma for governments and international organisations. On the one hand the possibility of remaining anonymous is essential if the fundamental rights to privacy and freedom of expression are to be maintained in cyberspace. On the other hand the ability to participate and communicate on-line without revealing one's identity runs against the grain of initiatives being developed to support other key areas of public policy, such as the fight against illegal and harmful content, financial fraud or copyright infringements. Of course such apparent con-

49 "Large-scale exploratory or general surveillance must be forbidden···the most effective means to reduce unacceptable risks to privacy while recognising the needs for effective law enforcement is that traffic data should in principle not be kept only for law enforcement purposes and that national laws should not oblige telecommunications operators, telecommunications service and Internet Service providers to keep traffic data for a period of time longer than necessary for billing purposes," Recommendation 3/99 of the Art. 29 Data Protection Working Party of 7 September 1999, http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

50 As incorporated in the European Convention on Human Rights (Article 8, right to privacy), the EU Charter on Fundamental Rights, the EU Treaty and EC Data Protection Directives.

51 http://www.linx.net/noncore/bcp/.

52 Working Party on the Protection of Individuals with regard to the Processing of Personal data. Recommendation 3/97 Anonymity on the Internet. Adopted by the Working Party on 3 December 1997. http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

flict between different public policy objectives is not new. In the context of the more traditional off-line modes of communication, such as letter and parcel post, the telephone, newspapers, or broadcasting via radio and television, a balance between these objectives has been achieved. The challenge facing policy-makers today is to ensure that this balanced approach, which guarantees basic rights while permitting proportionate restrictions to these rights in limited and specified circumstances, is maintained in the new context of cyberspace. Central to this balance will be the extent of, and limits to, a person's ability to participate on-line in an anonymous fashion.

In the concluding Declaration of the Ministerial Conference in Bonn on Global Information Networks, 6-8 July 1997, it was stated that the principle should be that where the user can choose to remain anonymous off-line, that choice should also be available on-line. There is a clear consensus therefore that activity on networks should be viewed using the basic legal principles that apply elsewhere. The Internet is not an anarchic ghetto where society's rules do not apply. Equally, though, the ability of governments and public authorities to restrict the rights of individuals and monitor potentially unlawful behaviour should be no greater on public networks than it is in the outside, off-line world. The requirement that restrictions to fundamental rights and freedoms be properly justified, necessary and proportional in view of other public policy objectives, must also apply in cyberspace.

In the Article 29 Data Protection Working Party recommendation it is indicated in detail how this may be achieved in specific cases (for example concerning e-mail, newsgroups, etc).[53] The Commission shares the views expressed by the Working Party.

5.4. Practical co-operation at international level

In the recent past, world-wide combined law enforcement operations, such as Operations Starburst and Cathedral against paedophile rings, have shown the value of co-ordinated international action by law enforcement and judiciary, both in exchanging information at the preliminary stage and in preventing the tipping off of other ring members when arrests and seizures are made. The Internet has also proved to be a valuable and efficient tool for police and customs investigations where it is used as an instrument for committing traditional crimes, such as counterfeiting and smuggling.On the other hand, these operations have also revealed the major legal and operational difficulties with which law enforcement and judiciary were confronted while managing this action, such as preparation of cross border evidence or commission rogatoire, victim identification, and the role of intergovernmental organisations dealing with police issues (Interpol and Europol in particular).

In the field of practical international co-operation measures international networks for the exchange of information are becoming increasingly important for police and customs authorities.

Within the G8, a 24 hour/7 day information network of law-enforcement points of contact has been established and is already operational. Its main purpose is to receive and respond to urgent requests for co-operation in cases involving electronic evidence. The network has been used successfully in a number of cases. The EU JHA Council on 19 March 1998 endorsed the 10 Principles to combat high-tech crime adopted by the G8 and invited the non-G8 Countries of the Member States of the EU to join the network.[54] These contact points should co-operate directly, supplementing existing structures of mutual assistance and channels for communications.[55]

Creation of such a network is also foreseen by the draft C.o.E. Convention. Reference to a 24h/7d network of points of contact exists also in the Council Decision on combating Child Pornography on the Internet and in the EU Common Position on the draft C.o.E. Convention on cyber-crime[56] and in the Council decision endorsing the G8 action plan,[57] but no concrete EU-specific initiatives have yet been taken.

The Commission considers that given the need for

53 http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

54 Apart from the G8 Members, five EU Member States have so far joined the G8 24/7 network.

55 At the World Conference against Commercial Sexual Exploitation of Children in Stockholm on 28 August 1996 proposals were made to include INTERPOL in the mentioned networks. The Decision of the EU Council on combating child pornography on the Internet foresees also the involvement of Europol in this field.

56 Article 1.4 of the Common Position: "Member States should support the establishment of provisions, which will facilitate international co-operation including provisions concerning mutual legal assistance to the widest extent possible. The Convention should facilitate the swift co-operation regarding computer-related and computer-aided offences. This form of co-operation may include the setting of 24-hour law enforcement points of contact, which supplement existing structures of mutual assistance."

57 Available on the European Judicial Network website http://ue.eu.int/ejn/index.htm.

appropriate expertise and expedited action in this field, the Council's intentions should be implemented without delay. To be successful, however, such a network would require both legally and technically literate staff, which implies appropriate training.

There is a similar need to intensify co-operation and information exchange between customs authorities. Existing forms of co-operation should be enhanced, and new means of managing joint operations and exchanging information should be developed. With due regard to data protection requirements, there is a growing consensus among customs authorities that international information networks should be formed to further facilitate the exchange of information. There is also a need for greater resources to be invested in this area, both regarding the upgrade of computer systems but also in educating personnel, in order for customs authorities to perform their duties more effectively.

5.5. Procedural law powers and jurisdiction

At the domestic level, and once the necessary conditions enshrined in law are fulfilled, law-enforcement authorities need to be able to search and seize data stored in computers speedily enough to prevent the destruction of criminal evidence. Law-enforcement authorities consider that they should have sufficient coercive powers to be able, within their jurisdiction, to search computer systems and seize data, order persons to submit specified computer data, order or obtain the expeditious preservation of specific data in accordance with normal legal safeguards and procedures. At present, however, the safeguards and procedures are not approximated.

Questions may arise if, when accessing a computer, law-enforcement authorities find that a number of computers and networks are involved which are located all over the country. Issues become much more complicated if, while searching a computer or simply pursuing an investigation, a law-enforcement authority finds itself accessing or needing to access data located in one or more different countries. Important sovereignty, human rights and law-enforcement interests are at stake and need to be balanced.

Existing legal tools for international co-operation in criminal law matters, i.e., mutual legal assistance, may not be appropriate or sufficient, since their implementation normally takes several days, weeks or months. There is a need for a mechanism by which countries can investigate offences and obtain evidence quickly and efficiently, or at least not lose important evidence in cross-border law-enforcement procedures, in a manner consistent with principles of national sovereignty and constitutional and human rights, including privacy and data protection.

New proposals under consideration in the Council of Europe draft Convention on Cybercrime to address these problems include orders for the preservation of data to assist specific investigations. However, other issues, such as transborder search and seizure, present difficult and as yet unresolved policy questions. More discussion among all parties concerned is clearly required before any concrete initiatives may be envisaged.

The G8 high-tech crime subgroup has discussed the issue of transborder search and seizure and, in anticipation of a subsequent more permanent agreement, has reached consensus on provisional principles[58]. Important questions, however, related in particular to when expedited search and seizure in particular situations is possible prior to informing the searched state, and appropriate safeguards to respect fundamental rights will need to be established. In the EU Common Position relating to the C.o.E. Draft Convention on Cybercrime, the Ministers have adopted an open-ended position.[59]

In transborder computer-related crime cases, it is also important that there are clear rules on which country has jurisdiction for prosecution. In particular it should be avoided that no country has jurisdiction. The main rules proposed by the draft Council of Europe Convention are that jurisdiction be established by a state when the offence is committed in its territory or by one of its nationals. When more than one state claims jurisdiction, the states concerned should consult with a view to determining the most appropriate jurisdiction. However, a lot will depend on effective bilateral or multilateral consultation. The Commission will keep this issue under review to see whether any further action may be required at EU level.

---

58 Communiqué of the Ministerial Conference of the G8 Countries on Combating Transnational Organised Crime-Moscow, 19-20 October 1999 (see http://www.usdoj.gov/criminal/cybercrime/action.htm and also http://www.usdoj.gov/criminal/cybercrime/principles.htm).

59 OJ L 142/2: "Subject to constitutional principles and specific safeguards in order to respect appropriately the sovereignty, security, public policy or other essential interests of other States, a transborder computer search for the purpose of the investigation of a serious criminal offence, to be further defined in the Convention, may be considered in exceptional cases, and in particular where there is an emergency, for example, as far as necessary to prevent the commission of an offence that is likely to result in the death of or serious injury to a person."

The Commission, having participated in both the C.o.E. and the G8 discussions, recognises the complexity and difficulties associated with procedural law issues. But effective co-operation within the EU to combat cybercrime is an essential element of a safer Information Society and the establishment of an Area of Freedom, Security and Justice.

The Commission intends to continue its consultations with all parties concerned over the coming months with a view to building on this work. This issue will also be considered in the wider context of its work on implementing the conclusions of the European Council in Tampere in October 1999. In particular, the Tampere Summit asked the Council and the Commission to adopt, by December 2000, a programme of measures to implement the principle of mutual recognition of judicial decisions. The Commission has already published a Communication on Mutual Recognition of Final Decisions in Criminal Matters.[60] As part of its contribution to implementing the part of the programme of measures dealing with enforcement of pre-trial orders, the Commission will consider the options for mutual recognition of pre-trial orders associated with cybercrime investigations with a view to bringing forward a legislative proposal under Title VI of the TEU.

5.6. Evidential validity of computer data

Even in cases in which law-enforcement authorities have accessed computer data which seem to be criminal evidence, they need to be able to retrieve and authenticate them for use in criminal investigations and prosecutions. This is not a very easy task given the volatile nature and ease of manipulation, falsification, technological protection or deletion of electronic data. It is addressed by computer forensics, which encompasses the development and use of scientific protocols and procedures for searching computers and analysing and maintaining the authenticity of data that has been retrieved.

At the request of the G8 experts, the International Organisation of Computer Evidence (IOCE) has agreed to develop recommendations for standards, including the definition of common terms, identification methods and techniques to be used and establishment of a common format for forensic requests. The EU should be associated with this work, both at the level of Member States specialised computer-crime investigation bodies and through the R&D supported by the 5th Framework Programme (IST Programme).

60 COM (2000) 495, Brussels 26.7.2000.

6. NON-LEGISLATIVE MEASURES

Appropriate legislation at both national and international level is necessary but not in itself sufficient for effectively combating computer-related crime and network misuse. A number of supplementary, non-legislative conditions are also required to complement the legislative measures. Most have been included in the recommendations of the COMCRIME study, the G8 has proposed such in its 10-point action plan and they have received broad support in the informal consultation process that preceded the drafting of this Communication. They include:

- the creation of special computer-crime police units at the national level, where they do not already exist;
- improved co-operation between law enforcement, industry, consumer organisations and data protection authorities;
- encouraging appropriate industry and community-led initiatives, including on security products.

The issue of encryption is likely to remain important in this context. Encryption is an essential tool to facilitate the implementation and adoption of new services, including electronic commerce, and can make a substantial contribution to the prevention of crime on the Internet. The Commission's policy on encryption has been laid down in its Communication on trust and confidence in electronic communication of 1997,[61] in which the Commission indicated that it would try to abolish all restrictions on the free circulation of all encryption products at the level of the European Community. The Communication further stated that domestic restrictions on the free circulation of encryption products have to be compatible with Community law and that it will examine whether such national restrictions are justified and proportionate, notably with respect to the free circulation provisions of the Treaty, the case law of the Court of Justice and the requirements of the Data Protection Directives. Nevertheless, the Commission recognises that encryption also presents new and difficult challenges for law enforcement agencies.

The Commission therefore welcomes the recently adopted revised dual-use goods regulation that significantly contributed to liberalise the availability of encryption products, while recognising that this needs to be accompanied by a better dialogue between users, industry and law enforcement. For its part, the Commission intends to promote this dia-

61 COM(97)503.

logue at EU level through the proposed EU Forum. The EU wide availability of security products, including strong encryption products, where appropriate certified to agreed evaluation criteria, would improve both crime prevention possibilities and users' trust in information society processes.

6.1. Specialised units at the national level

Given the technical and legal complexity of some of the computer-related criminal acts, the setting up of specialised units at national level is essential. Such specialised units, consisting of knowledgeable, multidisciplinary (law enforcement and judiciary) personnel should be equipped with adequate technical facilities and operate as rapid contact points for the purposes of:

- responding quickly to requests for information on suspected offences. Common formats for the exchange of such information will need to be defined, although discussions at G8 experts level have shown that this may not be an easy task, given differences in national legal cultures;
- acting as the law enforcement-interface nationally and internationally for hotlines[62] receiving complaints about illegal content from Internet users;
- improving and/or developing specialised computer investigation techniques for the purpose of detecting, investigating and prosecuting computer-related crimes;
- acting as a centre of excellence on cybercrime issues for the purpose of sharing best practices and experience.

Within the EU some Member States have already set up these specialised units dealing specifically with computer-related crimes. The Commission considers that the setting up of such specialised units is a Members State prerogative and strongly encourages Member States to take steps in that direction. Purchasing the latest hardware and software for these units and training their personnel involves substantial cost and presupposes priorities and political decisions at appropriate government levels.[63] The experience of already existing Member States units may be particularly valuable. The Commission will encourage the exchange of such experience.

The Commission also believes that Europol can provide further added value at EU level through co-ordination, analysis and other assistance to the national specialised units. The Commission will therefore support the extension of Europol's remit to cover cybercrime.

6.2. Specialised training

A considerable effort is required in the area of continuous, specialised training of both police and judicial staff. Computer-related criminal techniques and capabilities change more rapidly than those in more traditional areas of criminal activity.

Some Member States have been implementing initiatives for the high-tech training of law enforcement staff. They could provide advice and guidance to Member States that have not yet taken similar steps.

Individual projects aiming to achieve this - taking the form of exchanges of experiences, seminars on common challenges faced by the relevant professional categories- have been launched with the support of programmes administered by the Commission (in particular STOP, FALCONE and GROTIUS Programmes). The Commission will propose more activities in this area, including computer and online training.

Europol has taken the initiative to host a one-week training session for law-enforcement personnel from the Member States in November 2000, with particular reference to child pornography issues. The scope of such a session could be extended to include computer-related crime in general. Interpol has also been active in this field since a number of years. Its relevant initiatives could be extended to include a larger number of trainees.

62 So far, hotlines exist only in a limited number of countries. Examples are Cybertipline in the US and Internet Watch Foundation (IWF) in the UK, which, since Dec. 1996, has operated a telephone and e-mail hotline for members of the public to report material encountered on the Internet, which they consider illegal. The IWF judges whether the material is illegal, informs the ISPs and the police. Other monitoring bodies exist also in Norway (Redd Barna), the NL (Meldpunt), Germany (Newswatch, FSM and Jugendschutz), Austria (ISPAA) and Ireland (ISPAI). In the framework of the EU Daphne Programme, Childnet International is currently undertaken a project directly related to this issue ("International Hotline Providers in Europe Forum"). The UNESCO Expert Meeting in Paris in January 1999 supports and encourages also national hotlines and the creation of networks of hotlines or an international "electronic watchtower."

63 On the U.S. experience on this issue, see Michael A. Sussmann "The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium," Duke Journal of Comparative and International Law, Vol. 9 Spring 1999, p. 464.

The G8 has organised initiatives allowing the exchange of experience amongst law enforcement authorities and the establishment of common investigation techniques on the basis of concrete cases. A further initiative in the field of training is expected to be taken in the second half of year 2001. EU Member States participating in the G8 could share these experiences with the other Member States.

In the specific field of combating child pornography on the Internet, the creation and maintenance of a digital Central Library of child pornography images at an international level (to be made available on the Internet for specialised law enforcement units at national level, with the necessary conditions and limitations as regards access and protection of privacy) would aid the search for victims and perpetrators, help determine the nature of offences and train specialised police officers.[64]

6.3. Improved information and common rules for record keeping

The creation of a harmonised set of rules for police and judicial record-keeping and of the appropriate tools for statistical analysis of computer crime would help law enforcement and judicial authorities to better store, analyse, evaluate the formal information gathered in this still changing area.

Also, from the point of view of the private sector, such statistics are required for a proper assessment of the risks involved, and a cost-benefit analysis of their management. This is important not only for operational reasons (such as deciding on what security measures to take) but also for insurance purposes.

A database on computer crime statutes that was provided as part of the COMCRIME study, is being updated and made accessible to the Commission. The Commission will consider improving the content (include laws, court cases and literature) and usability of the database.

6.4. Co-operation between the various actors: the EU Forum

Effective co-operation between government and industry within the legal framework has been considered as an essential element of any public policy to tackle computer-related crimes.[65] Law-enforcement representatives have admitted that they have not always been sufficiently clear and precise on what they need from service providers. Industry representatives have expressed a generally positive attitude towards better co-operation with law enforcement whilst underlining the need for an appropriate balance between the protection of the fundamental rights and freedoms of citizens, in particular their right to privacy,[66] the need of combating crime and the economic burdens placed on providers.

Together, industry and law enforcement can raise public awareness on the risks posed by criminals on the Internet, promote best practices for security, and develop effective counter-crime tools and procedures. There have already been relevant initiatives in a number of Member States of which the UK Internet Crime Forum is probably the oldest and most far-reaching.[67]

The Commission welcomes these initiatives and considers they need to be encouraged in all Member States. The Commission intends to establish an EU Forum in which law enforcement agencies, Internet Service Providers, telecommunications operators, civil liberties organisations, consumer representatives, data protection authorities and other interested parties will be brought together

64 In this context, the project "Excalibur" developed by the Swedish National Crime Intelligence Division and co-sponsored by the European Commission under the STOP Programme has been a very successful initiative. This project has been set up with the co-operation of police forces from Germany, UK, the Netherlands and Belgium, together with Europol and Interpol. Other projects undertaken by the German BKA (the so-called "Perkeo") and the French Ministry of Interior ("Surfimage" project also co-sponsored under the STOP Programme) have also to be taken into right account.

65 In the Communiqué adopted in Washington on 9/10 December 1997 on Principles and 10 Points Action Plan to combat high-tech crime, G8 Ministers of Justice and of the Interior declared that: "it is the industrial sector that is designing, deploying and maintaining these global networks and is primarily responsible for the development of technical standards. Thus, it is incumbent on the industrial sector to play its part in developing and distributing secure systems designed to help detect computer abuse, preserve electronic evidence and assist in ascertaining the location and identity of criminals." The Decision of the EU Council to combat child pornography on the Internet underlines the need that Member States have a constructive dialogue with industry, and in contact with it, shall co-operate by sharing their experiences.

66 As set out in the EU Data Protection Directives, the Council of Europe Convention on Human Rights and the Council of Europe Convention no 108 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and relevant national law.

67 Established in 1997, the Internet Crime Forum includes police officers, Home Office and data protection officials and Internet industry representatives; it has plenary meetings 3-4 times a year and a number of permanent working groups.

with the aim of fully enhancing co-operation at EU level. At a first stage, this will include public officials to be named by Member States, technology experts, privacy experts to be appointed by the Art. 29 Data Protection Working Party and industry and consumer representatives to be identified in close consultation with industry and consumers associations. At a later stage, this Forum will include representatives from relevant national initiatives.

The EU Forum will be operated in an open and transparent manner, and relevant documents will be published on a website, and comments will be invited from all interested parties.

The EU Forum will be invited to consider in particular the following areas:

- Developing, where appropriate, 24-hours points of contact between government and industry;
- Developing an appropriate standard format for law enforcement requests for information from industry, increasing law enforcement's use of the Internet when communicating with service providers;
- Encouraging the development and/or implementation of codes of conduct and best practices and the sharing of such codes among industries and governments[68];
- Encouraging the exchange of information on trends in high-tech crime between the various parties, particularly industry and law enforcement agencies;
- Exploring law enforcement concerns in the development of new technologies;
- Encouraging further development of early warning and crisis management mechanisms to prevent, identify and handle threats or disrupting events on information infrastructures;
- Providing, where required, an enhanced expert contribution to work underway within the Council and in other international fora, for example the Council of Europe and G8;
- Encouraging co-operation between interested parties including principles shared by law enforcement, industry and users (e.g., Memorandum of Understanding (MOU), Codes of Practice in line with the legal framework).

6.5. Direct industry actions

To a large extent, combating computer-related crime is in the wider community's own interest. If consumers are to have confidence in electronic commerce, measures to prevent computer-related crime need to be an accepted element of good business practice. Many industries, e.g. in the banking, electronic communications, credit card and copyright sectors, and their customers are potential victims of computer-related crime. Companies naturally protect their own names and trademarks, and consequently have a role in fraud prevention. Organisations representing the software and audio industries (e.g., British Phonographic Industry - BPI) have teams investigating piracy (including Internet-related piracy). Internet service providers in a number of Member States have set up hot-lines for the reporting of illegal and harmful content.

The Commission has been supporting some of these initiatives by encouraging their participation in the EU R&D Framework Programme, the Internet Action Plan[69] and Title VI Programmes such as STOP and DAPHNE.

Best practice in these areas will be exchanged in the context of the EU Forum.

6.6. EU-supported RTD projects

In the Information Society Technologies (IST) RTD Programme, which is part of the 5th Framework Programme, 1998 to 2002, emphasis is put on the development and deployment of confidence-building technologies. As such, confidence-building technologies embrace both information and network security technologies as well as technical tools and methods to protect from abuses of the fundamental right to privacy and data protection and other personal rights and to fight computer crime.

The IST Programme, in particular work related to Information and network security and other confidence-building technologies in Key Action 2 - New Methods of Work and Electronic Commerce, provides the framework to develop capability and technologies to understand and tackle the emerging

68 As far as codes of conduct in the sense of Article 27 of Directive 95/46/EC are concerned (they could cover for example issues falling under Directive 97/66/EC such as interceptions), the Article 29 Data Protection Working Party and national data protection supervisory authorities are involved.

69 More information about the Internet Action Plan: Action Plan on Promoting Safer Use of the Internet is available at http://158.169.50.95:10080/iap/.

technology challenges related to preventing and combating computer crime and assure that security and privacy requirements can be met at EU level, at the level of virtual communities and at the level of the individual.

In addition, in order to properly deal with the challenges related to trust and confidence, including preventing and investigating computer crime, a dependability initiative has also been launched in the context of the IST Programme. The role of this initiative is to contribute towards raising and assuring trust and confidence in highly inter-linked information infrastructures and in tightly networked, embedded systems by promoting dependability awareness and dependability-enabling technologies. An integral part of this initiative is international co-operation. The IST Programme has developed working relationships with DARPA and NSF and established, in collaboration with the Department of State, the Joint Task Force on the Critical Infrastructure Protection under the auspices of the EC/US Joint Consultative Group of the S&T Co-operation Agreement.[70]

The Commission's Joint Research Centre (JRC), which has been supporting the dependability initiative in the IST Programme, will focus its efforts on developing appropriate and harmonised measures, indicators and statistics in consultation with other interested parties, including Europol. This will have the aim of developing a proper classification and understanding of illegal activities, their geographical distribution, their rate of increase and the effectiveness of measures taken to counteract them. Where appropriate, the JRC will involve other research groups and integrate their efforts and results. It will maintain an Internet web-site on the issue and report its progress to the EU Forum.

7. CONCLUSIONS AND PROPOSALS

Preventing and effectively combating computer-related crime presupposes the existence of a number of necessary conditions:

- the availability of preventive technologies. This requires an appropriate regulatory environment which gives room and incentives for innovation and research. Public financing can be justified to support the development and deployment of appropriate security technologies.
- the awareness of potential security risks and ways to combat them;
- adequate substantive and procedural legislative provisions, as regards both domestic and transnational criminal activities. National substantive criminal laws should be sufficiently comprehensive and effective in criminalising serious computer-related abuses and provide for dissuasive sanctions, helping to overcome dual criminality[71] problems and facilitating international co-operation. Where there is a well-founded need for action by law enforcement to expeditedly search, seize and securely copy computer data within their national territory in order to be able to investigate a computer related crime, this should be made possible by procedural laws, in conformity with the principles and exceptions provided for by Community law and in accordance with the European Convention on Human Rights.The Commission believes that the agreement reached on the interception provisions in the Convention on Mutual Assistance in Criminal Matters is the maximum possible that is achievable at present. The Commission will keep reviewing its implementation with Member States, industry and users to ensure that relevant initiatives are effective, transparent and well balanced;
- the availability of a sufficient number of well trained and equipped law-enforcement personnel. Close collaboration with Internet service providers and telecommunications operators in the field of training will be further encouraged;
- improved co-operation between all the actors concerned; users and consumers, industry, law enforcement and data protection authorities. This is critical to investigating computer crime and protecting public safety. Industry needs to operate within clear rules and obligations. Governments should recognise that the needs of law enforcement may place burdens on industry and thus take reasonable steps to minimise such burdens. At the same time, industry ought to include public safety considerations in its business practices. Increasingly this will need the active co-operation and support of the individual user and consumer;

70 More information about the IST Programme is available at http://www.cordis.lu/ist.

71 Where criminal investigations necessitate the assistance of authorities in other countries, many legal systems require that the crime is punishable in both countries as a prerequisite for certain types of mutual legal assistance and for extradition.

- continuous industry and community-led initiatives. Hotlines, already in place for reporting illegal and harmful content cases, may be extended to other types of abuse. Industry self-regulation and a multidisciplinary memorandum of understanding could involve the broadest possible number of interested parties and play a multiple role in helping prevent and combat computer crime and increasing awareness and trust;
- the achievements and potential of R&D should be exploited to the maximum extent possible. The strategic focus will be on bringing together affordable and effective security and other confidence building technology developments and EU policy initiatives.

Any measures to be agreed by the EU, however, should take into account the need to gradually bring the candidate countries into the realms of EU and international co-operation in this field and avoid that they are used as computer crime havens. Involvement of representatives of these countries in some or all of the relevant EU meetings should be considered.

The Commission proposals can be divided into the following areas.

7.1. Legislative proposals

The Commission will bring forward legislative proposals under the Title VI of the TEU:

- to approximate Member States' laws in the area of child pornography offences. This initiative will be part of a package of proposals which will also cover wider issues associated with the sexual exploitation of children and trafficking in human beings, as announced in the Commission's Communication on trafficking in human beings of December 1998. Such a proposal will be fully in line with the European Parliament's attempt to turn the Austrian initiative for a Council Decision on child pornography into a Framework Decision requiring approximation of laws. This is also consistent with the Tampere conclusions and the EU strategy for the new Millennium to combat organised crime. This is already part of the Scoreboard for the establishment of an area of Freedom, Security and Justice.
- to further approximate substantive criminal law in the area of high-tech crime. This will include offences related to hacking and denial of service attacks. The Commission will also examine the scope for action against racism and xenophobia on the Internet with a view to bringing forward a Framework Decision under Title VI of the TEU covering both off-line and on-line racist and xenophobic activity. Finally, the problem of illicit drugs on the Internet will also be examined.
- to apply the principle of mutual recognition to pre-trial orders associated with cybercrime investigations and to facilitate computer-related criminal investigations involving more than one Member State with appropriate safeguards concerning fundamental rights. This proposal is consistent with the outline programme of measures for mutual recognition, which refers to the need to consider proposals on the production and freezing of evidence.

The need to take any measures, in particular of a legislative nature on the question of retention of traffic data will be assessed by the Commission amongst other consultations, on the basis of the outcome of the work that will be done by the proposed EU Forum in this area.

7.2. Non-legislative proposals

Action is proposed in a number of areas:

- the Commission will establish and chair an EU Forum in which law enforcement agencies, service providers, network operators, consumer groups and data protection authorities will be brought together with the aim of enhancing co-operation at EU level by raising public awareness on the risks posed by criminals on the Internet, promoting best practices for IT security, developing effective counter-crime tools and procedures to combat computer-related crime as well as encouraging further development of early warning and crisis management mechanisms. This would be an EU version of similar successful fora which exist in certain Member States. Where such fora do not exist the Commission would encourage Member States to set them up. Co-operation between these various fora would be encouraged and facilitated through the EU Forum.
- the Commission will continue to promote security and trust in the context of the eEurope initiative, the Internet Action Plan, the IST programme and the next framework programme for RTD. These will include pro-

moting the availability of products and services with an appropriate level of security and encouragement of a more liberalised use of strong encryption through a dialogue amongst all interested parties.

- the Commission will promote further projects under existing programmes to support the training of law enforcement staff on high-tech crime issues and to support research in forensic computing.
- the Commission will consider providing funding for improving the content and usability of the database of Member States' national laws provided by the COMCRIME study, and will launch a study to obtain a better picture of the nature and extent of computer-related crime in the Member States.

7.3 Action in other international fora

The Commission will continue to play a full role in ensuring co-ordination between Member States in other international fora in which cybercrime is being discussed such as the Council of Europe and G8. The Commission's initiatives at EU level will take full account of progress in other international fora, while seeking to achieve approximation within the EU.

Council Resolution of 3 October 2000 on the organisation and management of the Internet (2000/C 293/02)

THE COUNCIL OF THE EUROPEAN UNION,

1. RECALLING:
   - the Final Declaration of the European Ministerial Conference held in Bonn (6 to 8 July 1997) referring in particular to the creation of an "*internationally recognised and transparent system of management of the Domain Name System*" comprising "*adequate European representation*";
   - the EU-US joint statement on electronic commerce (5 December 1997) emphasising in particular that the role of government was to "*provide a consistent and predictable legal framework, ···and to ensure adequate protection of public interest objectives such as privacy, intellectual property rights, prevention of fraud, consumer protection and public safety*";
   - that greater consideration for public policies and the pursuit of globalisation of the management of Internet addresses and domain names are key objectives for the European Union;
   - the importance of the development of electronic commerce, which will require efficient and transparent management of the resources represented by domain names and Internet Protocol (IP) addresses, in particular through the deployment of the next generation of addresses using the IPv6 standard;
2. WELCOMES:
   - the Commission communication of 11 April 2000 on the organisation and management of the Internet;
   - the concerted work already done by the Member States and the Commission in that context and the active involvement of Internet professionals and professionals from Europe's private sector in the setting up of the Internet Corporation for Assigned Names and Numbers (ICANN);

- the fact that ICANN's Governmental Advisory Committee (GAC) has authorised account to be taken of public policy goals and has defined a clear and balanced system for country code Top Level Domain names (ccTLD);
- the work undertaken in the relevant international organisations, notably the World Intellectual Property Organisation (WIPO) and the International Telecommunication Union (ITU);

3. NOTES:
   - that a number of significant advances have been made on the management of addresses and domain names, such as the global make-up of ICANN's Board of Directors, generating competition at the level of the registrars, setting up dispute-resolution machinery for generic Top Level Domain names (gTLDs);
   - that the reform of Internet management is nonetheless still going through a transitional phase, and consequently the objectives which the European Union has set itself on domain name management cannot be regarded as having been achieved;
   - that a number of important issues currently remain unresolved, in particular:
     - the nature of, and arrangements for, balanced and equal oversight of some of ICANN's activities by public authorities;
     - the rules to govern generic domains, notably database ownership and separation of registries' and registrars' activities;
     - the redelegation of certain ccTLDs to another manager at the request of the Government concerned;
     - regarding the relationships between the Registries established in the Community with their public authorities on the one hand and with ICANN on the other hand;
     - the transfer of the management of the root server system from the US Department of Commerce to ICANN, under appropriate international supervision by public authorities;
   - that those issues need to be addressed with due regard for both the interests of the international community as a whole and the public policy challenges involved, particularly as regards competition, personal data protection and respect for intellectual property rights;

4. ENCOURAGES:
   - the implementation of the principles adopted by the GAC;
   - WIPO to continue its work on the recognition of rights and the use of names in the Domain Name System. Furthermore WIPO is encouraged to develop, for the assistance of ccTLD administrators, voluntary guidelines for practices and policies to curb abusive and bad faith registration of protected names, and resolve related disputes;
   - the ITU to continue to take an active part in the international discussions and initiatives on the organisation and management of the Internet, especially on issues related to Internet addresses and protocols;

5. RESOLVES TO INVITE THE MEMBER STATES:
   - to consult each other with a view to establishing common European positions on the subject in the international bodies concerned and to securing genuine globalisation of Internet management;
   - to take due account of the policy objectives listed by the Commission communication in the Community's policies on the information society and on research and development;
   - to implement, in accordance with national provisions, the principles adopted by the GAC on domain name management;

6. RESOLVES TO INSTRUCT THE COMMISSION:
   - to encourage the coordination of policies on Internet management, in particular by defining an appropriate framework to organise and structure activities in this area;
   - to continue its efforts, in consultation with the Member States, to achieve genuine globalisation of Internet management with due regard for the imperatives of both public policies and international agreements;

- to set up a European network bringing together the scientific, technical and legal skills that currently exist in the Member States with regard to domain name, address and Internet protocol management.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof,

Having regard to the proposal from the Commission(1),

Having regard to the opinion of the Economic and Social Committee(2),

Acting in accordance with the procedure laid down in Article 251 of the Treaty(3),

Whereas:

(1) The European Union is seeking to forge ever closer links between the States and peoples of Europe, to ensure economic and social progress; in accordance with Article 14(2) of the Treaty, the internal market comprises an area without internal frontiers in which the free movements of goods, services and the freedom of establishment are ensured; the development of information society services within the area without internal frontiers is vital to eliminating the barriers which divide the European peoples.

(2) The development of electronic commerce within the information society offers significant employment opportunities in the Community, particularly in small and medium-sized enterprises, and will stimulate economic growth and investment in innovation by European companies, and can also enhance the competitiveness of European industry, provided that everyone has access to the Internet.

(3) Community law and the characteristics of the Community legal order are a vital asset to enable European citizens and operators to take full advantage, without consideration of borders, of the opportunities afforded by electronic commerce; this Directive therefore has the purpose of ensuring a high level of Community legal integration in order to establish a real area without internal borders for information society services.

(4) It is important to ensure that electronic commerce could fully benefit from the internal market and therefore that, as with Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities(4), a high level of Community integration is achieved.

(5) The development of information society services within the Community is hampered by a number of legal obstacles to the proper functioning of the internal market which make less attractive the exercise of the freedom of establishment and the freedom to provide services; these obstacles arise from divergences in legislation and from the legal uncertainty as to which national rules apply to such services; in the absence of coordination and adjustment of legislation in the relevant areas, obstacles might be justified in the light of the case-law of the Court of Justice of the European Communities; legal uncertainty exists with regard to the extent to which Member States may control services originating from another Member State.

(6) In the light of Community objectives, of Articles 43 and 49 of the Treaty and of secondary Community law, these obstacles should be eliminated by coordinating certain national laws and by clarifying certain legal concepts at Community level to the extent necessary for the proper functioning of the internal market; by dealing only with certain specific matters which give rise to problems for the internal market, this Directive is fully consistent with the need to respect the principle of subsidiarity as set out in Article 5 of the Treaty.

(7) In order to ensure legal certainty and consumer confidence, this Directive must lay down a clear and general framework to cover certain legal aspects of electronic commerce in the internal market.

(8) The objective of this Directive is to create a legal framework to ensure the free movement of information society services between Member States and not to harmonise the field of criminal law as such.

(9) The free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely freedom of expression as enshrined in Article 10(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, which has been ratified by all the Member States; for this reason, directives covering the supply of information society services must ensure that this activity may be engaged in freely in the light of that Article, subject only to the restrictions laid down in paragraph 2 of that Article and in Article 46(1) of the Treaty; this Directive is not intended to affect national fundamental rules and principles relating to freedom of expression.

(10) In accordance with the principle of proportionality, the measures provided for in this Directive are strictly limited to the minimum needed to achieve the objective of the proper functioning of the internal market; where action at Community level is necessary, and in order to guarantee an area which is truly without internal frontiers as far as electronic commerce is concerned, the Directive must ensure a high level of protection of objectives of general interest, in particular the protection of minors and human dignity, consumer protection and the protection of public health; according to Article 152 of the Treaty, the protection of public health is an essential component of other Community policies.

(11) This Directive is without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts; amongst others, Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts(5) and Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts(6) form a vital element for protecting consumers in contractual matters; those Directives also apply in their entirety to information society services; that same Community acquis, which is fully applicable to information society services, also embraces in particular Council Directive 84/450/EEC of 10 September 1984 concerning misleading and comparative advertising(7), Council Directive 87/102/EEC of 22 December 1986 for the approximation of the laws, regulations and administrative provisions of the Member States concerning consumer credit(8), Council Direc-

tive 93/22/EEC of 10 May 1993 on investment services in the securities field(9), Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours(10), Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer production in the indication of prices of products offered to consumers(11), Council Directive 92/59/EEC of 29 June 1992 on general product safety(12), Directive 94/47/EC of the European Parliament and of the Council of 26 October 1994 on the protection of purchasers in respect of certain aspects on contracts relating to the purchase of the right to use immovable properties on a timeshare basis(13), Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests(14), Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions concerning liability for defective products(15), Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees(16), the future Directive of the European Parliament and of the Council concerning the distance marketing of consumer financial services and Council Directive 92/28/EEC of 31 March 1992 on the advertising of medicinal products(17); this Directive should be without prejudice to Directive 98/43/EC of the European Parliament and of the Council of 6 July 1998 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the advertising and sponsorship of tobacco products(18) adopted within the framework of the internal market, or to directives on the protection of public health; this Directive complements information requirements established by the abovementioned Directives and in particular Directive 97/7/EC.

(12) It is necessary to exclude certain activities from the scope of this Directive, on the grounds that the freedom to provide services in these fields cannot, at this stage, be guaranteed under the Treaty or existing secondary legislation; excluding these activities does not preclude any instruments which might prove necessary for the proper functioning of the internal market; taxation, particularly value added tax imposed on a large number of the services covered by this Directive, must be excluded form the scope of this Directive.

(13) This Directive does not aim to establish rules on fiscal obligations nor does it pre-empt the drawing up of Community instruments concerning fiscal aspects of electronic commerce.

(14) The protection of individuals with regard to the processing of personal data is solely governed by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data(19) and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(20) which are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States; the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries; this Directive cannot prevent the anonymous use of open networks such as the Internet.

(15) The confidentiality of communications is guaranteed by Article 5 Directive 97/66/EC; in accordance with that Directive, Member States must prohibit any kind of interception or surveillance of such communications by others than the senders and receivers, except when legally authorised.

(16) The exclusion of gambling activities from the scope of application of this Directive covers only games of chance, lotteries and betting transactions, which involve wagering a stake with monetary value; this does not cover promotional competitions or games where the purpose is to encourage the sale of goods or services and where payments, if they arise, serve only to acquire the promoted goods or services.

(17) The definition of information society services already exists in Community law in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services(21) and in Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the

legal protection of services based on, or consisting of, conditional access(22); this definition covers any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service; those services referred to in the indicative list in Annex V to Directive 98/34/EC which do not imply data processing and storage are not covered by this definition.

(18) Information society services span a wide range of economic activities which take place on-line; these activities can, in particular, consist of selling goods on-line; activities such as the delivery of goods as such or the provision of services off-line are not covered; information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data; information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service; television broadcasting within the meaning of Directive EEC/89/552 and radio broadcasting are not information society services because they are not provided at individual request; by contrast, services which are transmitted point to point, such as video-on-demand or the provision of commercial communications by electronic mail are information society services; the use of electronic mail or equivalent individual communications for instance by natural persons acting outside their trade, business or profession including their use for the conclusion of contracts between such persons is not an information society service; the contractual relationship between an employee and his employer is not an information society service; activities which by their very nature cannot be carried out at a distance and by electronic means, such as the statutory auditing of company accounts or medical advice requiring the physical examination of a patient are not information society services.

(19) The place at which a service provider is established should be determined in conformity with the case-law of the Court of Justice according to which the concept of establishment involves the actual pursuit of an economic activity through a fixed establishment for an indefinite period; this requirement is also fulfilled where a company is constituted for a given period; the place of establishment of a company providing services via an Internet website is not the place at which the technology supporting its website is located or the place at which its website is accessible but the place where it pursues its economic activity; in cases where a provider has several places of establishment it is important to determine from which place of establishment the service concerned is provided; in cases where it is difficult to determine from which of several places of establishment a given service is provided, this is the place where the provider has the centre of his activities relating to this particular service.

(20) The definition of "recipient of a service" covers all types of usage of information society services, both by persons who provide information on open networks such as the Internet and by persons who seek information on the Internet for private or professional reasons.

(21) The scope of the coordinated field is without prejudice to future Community harmonisation relating to information society services and to future legislation adopted at national level in accordance with Community law; the coordinated field covers only requirements relating to on-line activities such as on-line information, on-line advertising, on-line shopping, on-line contracting and does not concern Member States' legal requirements relating to goods such as safety standards, labelling obligations, or liability for goods, or Member States' requirements relating to the delivery or the transport of goods, including the distribution of medicinal products; the coordinated field does not cover the exercise of rights of pre-emption by public authorities concerning certain goods such as works of art.

(22) Information society services should be supervised at the source of the activity, in order to ensure an effective protection of public interest objectives; to that end, it is necessary to ensure that the competent authority provides such protection not only for the citizens of its own country but for all Community citizens; in order to improve mutual trust between Member States, it is essential to state clearly this responsibility on the part of the Member State where the services originate; moreover, in order to effectively guarantee freedom to provide services and legal certainty for suppliers and recipients of services, such information society services

should in principle be subject to the law of the Member State in which the service provider is established.

(23) This Directive neither aims to establish additional rules on private international law relating to conflicts of law nor does it deal with the jurisdiction of Courts; provisions of the applicable law designated by rules of private international law must not restrict the freedom to provide information society services as established in this Directive.

(24) In the context of this Directive, notwithstanding the rule on the control at source of information society services, it is legitimate under the conditions established in this Directive for Member States to take measures to restrict the free movement of information society services.

(25) National courts, including civil courts, dealing with private law disputes can take measures to derogate from the freedom to provide information society services in conformity with conditions established in this Directive.

(26) Member States, in conformity with conditions established in this Directive, may apply their national rules on criminal law and criminal proceedings with a view to taking all investigative and other measures necessary for the detection and prosecution of criminal offences, without there being a need to notify such measures to the Commission.

(27) This Directive, together with the future Directive of the European Parliament and of the Council concerning the distance marketing of consumer financial services, contributes to the creating of a legal framework for the on-line provision of financial services; this Directive does not pre-empt future initiatives in the area of financial services in particular with regard to the harmonisation of rules of conduct in this field; the possibility for Member States, established in this Directive, under certain circumstances of restricting the freedom to provide information society services in order to protect consumers also covers measures in the area of financial services in particular measures aiming at protecting investors.

(28) The Member States' obligation not to subject access to the activity of an information society service provider to prior authorisation does not concern postal services covered by Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service(23) consisting of the physical delivery of a printed electronic mail message and does not affect voluntary accreditation systems, in particular for providers of electronic signature certification service.

(29) Commercial communications are essential for the financing of information society services and for developing a wide variety of new, charge-free services; in the interests of consumer protection and fair trading, commercial communications, including discounts, promotional offers and promotional competitions or games, must meet a number of transparency requirements; these requirements are without prejudice to Directive 97/7/EC; this Directive should not affect existing Directives on commercial communications, in particular Directive 98/43/EC.

(30) The sending of unsolicited commercial communications by electronic mail may be undesirable for consumers and information society service providers and may disrupt the smooth functioning of interactive networks; the question of consent by recipient of certain forms of unsolicited commercial communications is not addressed by this Directive, but has already been addressed, in particular, by Directive 97/7/EC and by Directive 97/66/EC; in Member States which authorise unsolicited commercial communications by electronic mail, the setting up of appropriate industry filtering initiatives should be encouraged and facilitated; in addition it is necessary that in any event unsolicited commercial communities are clearly identifiable as such in order to improve transparency and to facilitate the functioning of such industry initiatives; unsolicited commercial communications by electronic mail should not result in additional communication costs for the recipient.

(31) Member States which allow the sending of unsolicited commercial communications by electronic mail without prior consent of the recipient by service providers established in their territory have to ensure that the service providers consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

(32) In order to remove barriers to the development of cross-border services within the Community which members of the regulated professions might offer on the Internet, it is necessary that compliance be guaranteed at Community level

with professional rules aiming, in particular, to protect consumers or public health; codes of conduct at Community level would be the best means of determining the rules on professional ethics applicable to commercial communication; the drawing-up or, where appropriate, the adaptation of such rules should be encouraged without prejudice to the autonomy of professional bodies and associations.

(33) This Directive complements Community law and national law relating to regulated professions maintaining a coherent set of applicable rules in this field.

(34) Each Member State is to amend its legislation containing requirements, and in particular requirements as to form, which are likely to curb the use of contracts by electronic means; the examination of the legislation requiring such adjustment should be systematic and should cover all the necessary stages and acts of the contractual process, including the filing of the contract; the result of this amendment should be to make contracts concluded electronically workable; the legal effect of electronic signatures is dealt with by Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures(24); the acknowledgement of receipt by a service provider may take the form of the on-line provision of the service paid for.

(35) This Directive does not affect Member States' possibility of maintaining or establishing general or specific legal requirements for contracts which can be fulfilled by electronic means, in particular requirements concerning secure electronic signatures.

(36) Member States may maintain restrictions for the use of electronic contracts with regard to contracts requiring by law the involvement of courts, public authorities, or professions exercising public authority; this possibility also covers contracts which require the involvement of courts, public authorities, or professions exercising public authority in order to have an effect with regard to third parties as well as contracts requiring by law certification or attestation by a notary.

(37) Member States' obligation to remove obstacles to the use of electronic contracts concerns only obstacles resulting from legal requirements and not practical obstacles resulting from the impossibility of using electronic means in certain cases.

(38) Member States' obligation to remove obstacles to the use of electronic contracts is to be implemented in conformity with legal requirements for contracts enshrined in Community law.

(39) The exceptions to the provisions concerning the contracts concluded exclusively by electronic mail or by equivalent individual communications provided for by this Directive, in relation to information to be provided and the placing of orders, should not enable, as a result, the by-passing of those provisions by providers of information society services.

(40) Both existing and emerging disparities in Member States' legislation and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition; service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities; this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States; it is in the interest of all parties involved in the provision of information society services to adopt and implement such procedures; the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC and 97/66/EC.

(41) This Directive strikes a balance between the different interests at stake and establishes principles upon which industry agreements and standards can be based.

(42) The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider

has neither knowledge of nor control over the information which is transmitted or stored.

(43) A service provider can benefit from the exemptions for "mere conduit" and for "caching" when he is in no way involved with the information transmitted; this requires among other things that he does not modify the information that he transmits; this requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission.

(44) A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of "mere conduit" or "caching" and as a result cannot benefit from the liability exemptions established for these activities.

(45) The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.

(46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.

(47) Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.

(48) This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.

(49) Member States and the Commission are to encourage the drawing-up of codes of conduct; this is not to impair the voluntary nature of such codes and the possibility for interested parties of deciding freely whether to adhere to such codes.

(50) It is important that the proposed directive on the harmonisation of certain aspects of copyright and related rights in the information society and this Directive come into force within a similar time scale with a view to establishing a clear framework of rules relevant to the issue of liability of intermediaries for copyright and relating rights infringements at Community level.

(51) Each Member State should be required, where necessary, to amend any legislation which is liable to hamper the use of schemes for the out-of-court settlement of disputes through electronic channels; the result of this amendment must be to make the functioning of such schemes genuinely and effectively possible in law and in practice, even across borders.

(52) The effective exercise of the freedoms of the internal market makes it necessary to guarantee victims effective access to means of settling disputes; damage which may arise in connection with information society services is characterised both by its rapidity and by its geographical extent; in view of this specific character and the need to ensure that national authorities do not endanger the mutual confidence which they should have in one another, this Directive requests Member States to ensure that appropriate court actions are available; Member States should examine the need to provide access to judicial procedures by appropriate electronic means.

(53) Directive 98/27/EC, which is applicable to information society services, provides a mechanism relating to actions for an injunction aimed at the protection of the collective interests of consumers; this mechanism will contribute to the free movement of information society services by ensuring a high level of consumer protection.

(54) The sanctions provided for under this Directive are without prejudice to any other sanction or remedy provided under national law; Member States are not obliged to provide criminal sanctions for infringement of national provisions adopted pursuant to this Directive.

(55) This Directive does not affect the law applicable to contractual obligations relating to consumer contracts; accordingly, this Directive cannot have the result of depriving the consumer of the protection afforded to him by the mandatory rules relating to contractual obligations of the law of the Member State in which he has his habitual residence.

(56) As regards the derogation contained in this Directive regarding contractual obligations concerning contracts concluded by consumers, those obligations should be interpreted as including information on the essential elements of the content of the contract, including consumer rights, which have a determining influence on the decision to contract.

(57) The Court of Justice has consistently held that a Member State retains the right to take measures against a service provider that is established in another Member State but directs all or most of his activity to the territory of the first Member State if the choice of establishment was made with a view to evading the legislation that would have applied to the provider had he been established on the territory of the first Member State.

(58) This Directive should not apply to services supplied by service providers established in a third country; in view of the global dimension of electronic commerce, it is, however, appropriate to ensure that the Community rules are consistent with international rules; this Directive is without prejudice to the results of discussions within international organisations (amongst others WTO, OECD, Uncitral) on legal issues.

(59) Despite the global nature of electronic communications, coordination of national regulatory measures at European Union level is necessary in order to avoid fragmentation of the internal market, and for the establishment of an appropriate European regulatory framework; such coordination should also contribute to the establishment of a common and strong negotiating position in international forums.

(60) In order to allow the unhampered development of electronic commerce, the legal framework must be clear and simple, predictable and consistent with the rules applicable at international level so that it does not adversely affect the competitiveness of European industry or impede innovation in that sector.

(61) If the market is actually to operate by electronic means in the context of globalisation, the European Union and the major non-European areas need to consult each other with a view to making laws and procedures compatible.

(62) Cooperation with third countries should be strengthened in the area of electronic commerce, in particular with applicant countries, the developing countries and the European Union's other trading partners.

(63) The adoption of this Directive will not prevent the Member States from taking into account the various social, societal and cultural implications which are inherent in the advent of the information society; in particular it should not hinder measures which Member States might adopt in conformity with Community law to achieve social, cultural and democratic goals taking into account their linguistic diversity, national and regional specificities as well as their cultural heritage, and to ensure and maintain public access to the widest possible range of information society services; in any case, the development of the information society is to ensure that Community citizens can have access to the cultural European heritage provided in the digital environment.

(64) Electronic communication offers the Member States an excellent means of providing public services in the cultural, educational and linguistic fields.

(65) The Council, in its resolution of 19 January 1999 on the consumer dimension of the information society(25), stressed that the protection of consumers deserved special attention in this field; the Commission will examine the degree to which existing consumer protection rules provide insufficient protection in the context of the information society and will identify, where necessary, the deficiencies of this legislation and those issues which could require additional measures; if need be, the Commission should make specific additional proposals to resolve such deficiencies that will thereby have been identified,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I
GENERAL PROVISIONS

Article 1
Objective and scope

1. This Directive seeks to contribute to the proper

functioning of the internal market by ensuring the free movement of information society services between the Member States.

2. This Directive approximates, to the extent necessary for the achievement of the objective set out in paragraph 1, certain national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and cooperation between Member States.

3. This Directive complements Community law applicable to information society services without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts and national legislation implementing them in so far as this does not restrict the freedom to provide information society services.

4. This Directive does not establish additional rules on private international law nor does it deal with the jurisdiction of Courts.

5. This Directive shall not apply to:

   (a) the field of taxation;

   (b) questions relating to information society services covered by Directives 95/46/EC and 97/66/EC;

   (c) questions relating to agreements or practices governed by cartel law;

   (d) the following activities of information society services:

   - the activities of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority,
   - the representation of a client and defence of his interests before the courts,
   - gambling activities which involve wagering a stake with monetary value in games of chance, including lotteries and betting transactions.

6. This Directive does not affect measures taken at Community or national level, in the respect of Community law, in order to promote cultural and linguistic diversity and to ensure the defence of pluralism.

Article 2
Definitions

For the purpose of this Directive, the following terms shall bear the following meanings:

(a) "information society services": services within the meaning of Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC;

(b) "service provider": any natural or legal person providing an information society service;

(c) "established service provider": a service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider;

(d) "recipient of the service": any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible;

(e) "consumer": any natural person who is acting for purposes which are outside his or her trade, business or profession;

(f) "commercial communication": any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession. The following do not in themselves constitute commercial communications:

- information allowing direct access to the activity of the company, organisation or person, in particular a domain name or an electronic-mail address,
- communications relating to the goods, services or image of the company, organisation or person compiled in an independent manner, particularly when this is without financial consideration;

(g) "regulated profession": any profession within the meaning of either Article 1(d) of Council Directive 89/48/EEC of 21 December 1988 on a general system for the recognition of higher-education diplomas awarded on completion of professional education and training of at least three-years' duration(26) or of Article 1(f) of Council Directive 92/51/EEC of 18 June 1992 on a second general system for the recognition of

professional education and training to supplement Directive 89/48/EEC(27);

(h) "coordinated field": requirements laid down in Member States' legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them.

(i) The coordinated field concerns requirements with which the service provider has to comply in respect of:

- the taking up of the activity of an information society service, such as requirements concerning qualifications, authorisation or notification,
- the pursuit of the activity of an information society service, such as requirements concerning the behaviour of the service provider, requirements regarding the quality or content of the service including those applicable to advertising and contracts, or requirements concerning the liability of the service provider;

(ii) The coordinated field does not cover requirements such as:

- requirements applicable to goods as such,
- requirements applicable to the delivery of goods,
- requirements applicable to services not provided by electronic means.

Article 3
Internal market

1. Each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field.
2. Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State.
3. Paragraphs 1 and 2 shall not apply to the fields referred to in the Annex.
4. Member States may take measures to derogate from paragraph 2 in respect of a given information society service if the following conditions are fulfilled:

(a) the measures shall be:

(i) necessary for one of the following reasons:

- public policy, in particular the prevention, investigation, detection and prosecution of criminal offences, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons,
- the protection of public health,
- public security, including the safeguarding of national security and defence,
- the protection of consumers, including investors;

(ii) taken against a given information society service which prejudices the objectives referred to in point (i) or which presents a serious and grave risk of prejudice to those objectives;

(iii) proportionate to those objectives;

(b) before taking the measures in question and without prejudice to court proceedings, including preliminary proceedings and acts carried out in the framework of a criminal investigation, the Member State has:

- asked the Member State referred to in paragraph 1 to take measures and the latter did not take such measures, or they were inadequate,
- notified the Commission and the Member State referred to in paragraph 1 of its intention to take such measures.

5. Member States may, in the case of urgency, derogate from the conditions stipulated in paragraph 4(b). Where this is the case, the measures shall be notified in the shortest possible time to the Commission and to the Member State referred to in paragraph 1, indicating the reasons for which the Member State considers that there is urgency.
6. Without prejudice to the Member State's possibility of proceeding with the measures in question, the Commission shall examine the compatibility of the notified measures with

Community law in the shortest possible time; where it comes to the conclusion that the measure is incompatible with Community law, the Commission shall ask the Member State in question to refrain from taking any proposed measures or urgently to put an end to the measures in question.

CHAPTER II
PRINCIPLES

SECTION 1: ESTABLISHMENT AND INFORMATION REQUIREMENTS

Article 4
Principle excluding prior authorisation

1. Member States shall ensure that the taking up and pursuit of the activity of an information society service provider may not be made subject to prior authorisation or any other requirement having equivalent effect.

2. Paragraph 1 shall be without prejudice to authorisation schemes which are not specifically and exclusively targeted at information society services, or which are covered by Directive 97/13/EC of the European Parliament and of the Council of 10 April 1997 on a common framework for general authorisations and individual licences in the field of telecommunications services(28).

Article 5
General information to be provided

1. In addition to other information requirements established by Community law, Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information:

   (a) the name of the service provider;

   (b) the geographic address at which the service provider is established;

   (c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;

   (d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register;

   (e) where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority;

   (f) as concerns the regulated professions:

   - any professional body or similar institution with which the service provider is registered,
   - the professional title and the Member State where it has been granted,
   - a reference to the applicable professional rules in the Member State of establishment and the means to access them;

   (g) where the service provider undertakes an activity that is subject to VAT, the identification number referred to in Article 22(1) of the sixth Council Directive 77/388/EEC of 17 May 1977 on the harmonisation of the laws of the Member States relating to turnover taxes - Common system of value added tax: uniform basis of assessment(29).

2. In addition to other information requirements established by Community law, Member States shall at least ensure that, where information society services refer to prices, these are to be indicated clearly and unambiguously and, in particular, must indicate whether they are inclusive of tax and delivery costs.

SECTION 2: COMMERCIAL COMMUNICATIONS

Article 6
Information to be provided

In addition to other information requirements established by Community law, Member States shall ensure that commercial communications which are part of, or constitute, an information society service comply at least with the following conditions:

(a) the commercial communication shall be clearly identifiable as such;

(b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;

(c) promotional offers, such as discounts, premiums and gifts, where permitted in the Member State where the service provider is established,

shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously;

(d) promotional competitions or games, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously.

Article 7
Unsolicited commercial communication

1. In addition to other requirements established by Community law, Member States which permit unsolicited commercial communication by electronic mail shall ensure that such commercial communication by a service provider established in their territory shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient.

2. Without prejudice to Directive 97/7/EC and Directive 97/66/EC, Member States shall take measures to ensure 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.

Article 8
Regulated professions

1. Member States shall ensure that the use of commercial communications which are part of, or constitute, an information society service provided by a member of a regulated profession is permitted subject to compliance with the professional rules regarding, in particular, the independence, dignity and honour of the profession, professional secrecy and fairness towards clients and other members of the profession.

2. Without prejudice to the autonomy of professional bodies and associations, Member States and the Commission shall encourage professional associations and bodies to establish codes of conduct at Community level in order to determine the types of information that can be given for the purposes of commercial communication in conformity with the rules referred to in paragraph 1

3. When drawing up proposals for Community initiatives which may become necessary to ensure the proper functioning of the Internal Market with regard to the information referred to in paragraph 2, the Commission shall take due account of codes of conduct applicable at Community level and shall act in close cooperation with the relevant professional associations and bodies.

4. This Directive shall apply in addition to Community Directives concerning access to, and the exercise of, activities of the regulated professions.

SECTION 3: CONTRACTS CONCLUDED BY ELECTRONIC MEANS

Article 9
Treatment of contracts

1. Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means.

2. Member States may lay down that paragraph 1 shall not apply to all or certain contracts falling into one of the following categories:

   (a) contracts that create or transfer rights in real estate, except for rental rights;

   (b) contracts requiring by law the involvement of courts, public authorities or professions exercising public authority;

   (c) contracts of suretyship granted and on collateral securities furnished by persons acting for purposes outside their trade, business or profession;

   (d) contracts governed by family law or by the law of succession.

3. Member States shall indicate to the Commission the categories referred to in paragraph 2 to which they do not apply paragraph 1. Member States shall submit to the Commission every five years a report on the application of paragraph 2 explaining the reasons why they consider it necessary to maintain the category referred to in paragraph 2(b) to which they do not apply paragraph 1.

Article 10
Information to be provided

1. In addition to other information requirements established by Community law, Member States shall ensure, except when otherwise agreed by parties who are not consumers, that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service:

   a. the different technical steps to follow to conclude the contract;

   b. whether or not the concluded contract will be filed by the service provider and whether it will be accessible;

   c. the technical means for identifying and correcting input errors prior to the placing of the order;

   d. the languages offered for the conclusion of the contract.

2. Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider indicates any relevant codes of conduct to which he subscribes and information on how those codes can be consulted electronically.

3. Contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them.

4. Paragraphs 1 and 2 shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

Article 11
Placing of the order

1. Member States shall ensure, except when otherwise agreed by parties who are not consumers, that in cases where the recipient of the service places his order through technological means, the following principles apply:

   - the service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means,

   - the order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them.

2. Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider makes available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order.

3. Paragraph 1, first indent, and paragraph 2 shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

SECTION 4: LIABILITY OF INTERMEDIARY SERVICE PROVIDERS

Article 12
"Mere conduit"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

   (a) does not initiate the transmission;

   (b) does not select the receiver of the transmission; and

   (c) does not select or modify the information contained in the transmission.

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13
"Caching"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided

by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

(a) the provider does not modify the information;

(b) the provider complies with conditions on access to the information;

(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

(d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14
Hosting

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15
No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

CHAPTER III
IMPLEMENTATION

Article 16
Codes of conduct

1. Member States and the Commission shall encourage:

(a) the drawing up of codes of conduct at Community level, by trade, professional and consumer associations or organisations, designed to contribute to the proper implementation of Articles 5 to 15;

(b) the voluntary transmission of draft codes of conduct at national or Community level to the Commission;

(c) the accessibility of these codes of conduct in the Community languages by electronic means;

(d) the communication to the Member States and the Commission, by trade, professional and consumer associations or organisations, of their assessment of the application of their codes of conduct and their impact upon practices, habits or customs relating to electronic commerce;

(e) the drawing up of codes of conduct regarding the protection of minors and human dignity.

2. Member States and the Commission shall encourage the involvement of associations or organisations representing consumers in the drafting and implementation of codes of conduct affecting their interests and drawn up in accordance with paragraph 1(a). Where appropriate, to take account of their specific needs, associations representing the visually impaired and disabled should be consulted.

Article 17
Out-of-court dispute settlement

1. Member States shall ensure that, in the event of disagreement between an information society service provider and the recipient of the service, their legislation does not hamper the use of out-of-court schemes, available under national law, for dispute settlement, including appropriate electronic means.

2. Member States shall encourage bodies responsible for the out-of-court settlement of, in particular, consumer disputes to operate in a way which provides adequate procedural guarantees for the parties concerned.

3. Member States shall encourage bodies responsible for out-of-court dispute settlement to inform the Commission of the significant decisions they take regarding information society services and to transmit any other information on the practices, usages or customs relating to electronic commerce.

Article 18
Court actions

1. Member States shall ensure that court actions available under national law concerning information society services' activities allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.

2. The Annex to Directive 98/27/EC shall be supplemented as follows:

"11. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects on information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce) (OJ L 178, 17.7.2000, p. 1)."

Article 19
Cooperation

1. Member States shall have adequate means of supervision and investigation necessary to implement this Directive effectively and shall ensure that service providers supply them with the requisite information.

2. Member States shall cooperate with other Member States; they shall, to that end, appoint one or several contact points, whose details they shall communicate to the other Member States and to the Commission.

3. Member States shall, as quickly as possible, and in conformity with national law, provide the assistance and information requested by other Member States or by the Commission, including by appropriate electronic means.

4. Member States shall establish contact points which shall be accessible at least by electronic means and from which recipients and service providers may:

(a) obtain general information on contractual rights and obligations as well as on the complaint and redress mechanisms available in the event of disputes, including practical aspects involved in the use of such mechanisms;

(b) obtain the details of authorities, associations or organisations from which they may obtain further information or practical assistance.

5. Member States shall encourage the communication to the Commission of any significant administrative or judicial decisions taken in their territory regarding disputes relating to information society services and practices, usages and customs relating to electronic commerce. The Commission shall communicate these decisions to the other Member States.

Article 20
Sanctions

Member States shall determine the sanctions applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are enforced. The sanctions they provide for shall be effective, proportionate and dissuasive.

CHAPTER IV
FINAL PROVISIONS

Article 21
Re-examination

1. Before 17 July 2003, and thereafter every two years, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, accompanied, where necessary, by proposals for adapting it to legal, technical and economic developments in the field of information society services, in particular with respect to crime prevention, the protection of minors, consumer protection and to the proper functioning of the internal market.

2. In examining the need for an adaptation of this Directive, the report shall in particular analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services, "notice and take down" procedures and the attribution of liability following the taking down of content. The report shall also analyse the need for additional conditions for the exemption from liability, provided for in Articles 12 and 13, in the light of technical developments, and the possibility of applying the internal market principles to unsolicited commercial communications by electronic mail.

Article 22
Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 17 January 2002. They shall forthwith inform the Commission thereof.

2. When Member States adopt the measures referred to in paragraph 1, these shall contain a reference to this Directive or shall be accompanied by such reference at the time of their official publication. The methods of making such reference shall be laid down by Member States.

Article 23
Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 24
Addressees

This Directive is addressed to the Member States.

Done at Luxemburg, 8 June 2000.
For the European Parliament
The President N. Fontaine
For the Council
The President G. d'Oliveira Martins

[1] OJ C 30, 5.2.1999, p. 4.

[2] OJ C 169, 16.6.1999, p. 36.

[3] Opinion of the European Parliament of 6 May 1999 (OJ C 279, 1.10.1999, p. 389), Council common position of 28 February 2000 (OJ C 128, 8.5.2000, p. 32) and Decision of the European Parliament of 4 May 2000 (not yet published in the Official Journal).

[4] OJ L 298, 17.10.1989, p. 23. Directive as amended by Directive 97/36/EC of the European Parliament and of the Council (OJ L 202, 30.7.1997, p. 60).

[5] OJ L 95, 21.4.1993, p. 29.

[6] OJ L 144, 4.6.1999, p. 19.

[7] OJ L 250, 19.9.1984, p. 17. Directive as amended by Directive 97/55/EC of the European Parliament and of the Council (OJ L 290, 23.10.1997, p. 18).

[8] OJ L 42, 12.2.1987, p. 48. Directive as last amended by Directive 98/7/EC of the European Parliament and of the Council (OJ L 101, 1.4.1998, p. 17).

[9] OJ L 141, 11.6.1993, p. 27. Directive as last amended by Directive 97/9/EC of the European Parliament and of the Council (OJ L 84, 26.3.1997, p. 22).

[10] OJ L 158, 23.6.1990, p. 59.

[11] OJ L 80, 18.3.1998, p. 27.

[12] OJ L 228, 11.8.1992, p. 24.

[13] OJ L 280, 29.10.1994, p. 83.

[14] OJ L 166, 11.6.1998, p. 51. Directive as amended by Directive 1999/44/EC (OJ L 171, 7.7.1999, p. 12).

[15] OJ L 210, 7.8.1985, p. 29. Directive as amended by Directive 1999/34/EC (OJ L 141, 4.6.1999, p. 20).

[16] OJ L 171, 7.7.1999, p. 12.

[17] OJ L 113, 30.4.1992, p. 13.

[18] OJ L 213, 30.7.1998, p. 9.

[19] OJ L 281, 23.11.1995, p. 31.

[20] OJ L 24, 30.1.1998, p. 1.

[21] OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).

[22] OJ L 320, 28.11.1998, p. 54.

[23] OJ L 15, 21.1.1998, p. 14.

[24] OJ L 13, 19.1.2000, p. 12.

[25] OJ C 23, 28.1.1999, p. 1.

[26] OJ L 19, 24.1.1989, p. 16.

[27] OJ L 209, 24.7.1992, p. 25. Directive as last amended by Commission Directive 97/38/EC (OJ L 184, 12.7.1997, p. 31).

[28] OJ L 117, 7.5.1997, p. 15.

[29] OJ L 145, 13.6.1977, p. 1. Directive as last amended by Directive 1999/85/EC (OJ L 277, 28.10.1999, p. 34).

ANNEX

DEROGATIONS FROM ARTICLE 3

As provided for in Article 3(3), Article 3(1) and (2) do not apply to:

- copyright, neighbouring rights, rights referred to in Directive 87/54/EEC(1) and Directive 96/9/EC(2) as well as industrial property rights,
- the emission of electronic money by institutions in respect of which Member States have applied one of the derogations provided for in Article 8(1) of Directive 2000/46/EC(3),
- Article 44(2) of Directive 85/611/EEC(4),
- Article 30 and Title IV of Directive 92/49/EEC(5), Title IV of Directive 92/96/EEC(6), Articles 7 and 8 of Directive 88/357/EEC(7) and Article 4 of Directive 90/619/EEC(8),
- the freedom of the parties to choose the law applicable to their contract,
- contractual obligations concerning consumer contacts,
- formal validity of contracts creating or transferring rights in real estate where such contracts are subject to mandatory formal requirements of the law of the Member State where the real estate is situated,
- the permissibility of unsolicited commercial communications by electronic mail.

[1] OJ L 24, 27.1.1987, p. 36.

[2] OJ L 77, 27.3.1996, p. 20.

[3] Not yet published in the Official Journal.

[4] OJ L 375, 31.12.1985, p. 3. Directive as last amended by Directive 95/26/EC (OJ L 168, 18.7.1995, p. 7).

[5] OJ L 228, 11.8.1992, p. 1. Directive as last amended by Directive 95/26/EC.

[6] OJ L 360, 9.12.1992, p. 2. Directive as last amended by Directive 95/26/EC.

[7] OJ L 172, 4.7.1988, p. 1. Directive as last amended by Directive 92/49/EC.

[8] OJ L 330, 29.11.1990, p. 50. Directive as last amended by Directive 92/96/EC.

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 286 thereof,

Having regard to the proposal from the Commission(1),

Having regard to the opinion of the Economic and Social Committee(2),

Acting in accordance with the procedure laid down in Article 251 of the Treaty(3),

Whereas:

(1) Article 286 of the Treaty requires the application to the Community institutions and bodies of the Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data.

(2) A fully-fledged system of protection of personal data not only requires the establishment of rights for data subjects and obligations for those who process personal data, but also appropriate sanctions for offenders and monitoring by an independent supervisory body.

(3) Article 286(2) of the Treaty requires the establishment of an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies.

(4) Article 286(2) of the Treaty requires the adoption of any other relevant provisions as appropriate.

(5) A Regulation is necessary to provide the individual with legally enforceable rights, to specify the data processing obligations of the controllers within the Community institutions and bodies, and to create an independent supervisory authority responsible for monitoring the processing of personal data by the Community institutions and bodies.

(6) The Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up under Article 29 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data(4) has been consulted.

(7) The persons to be protected are those whose personal data are processed by Community institutions or bodies in any context whatsoever, for example because they are employed by those institutions or bodies.

(8) The principles of data protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely to be reasonably used either by the controller or by any other person to identify the said person. The principles of protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

(9) Directive 95/46/EC requires Member States to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, in order to ensure the free flow of personal data in the Community.

(10) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(5) specifies and adds to Directive 95/46/EC with respect to the processing of personal data in the telecommunications sector.

(11) Various other Community measures, including measures on mutual assistance between national authorities and the Commission, are also designed to specify and add to Directive 95/46/EC in the sectors to which they relate.

(12) Consistent and homogeneous application of

the rules for the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data should be ensured throughout the Community.

(13) The aim is to ensure both effective compliance with the rules governing the protection of individuals' fundamental rights and freedoms and the free flow of personal data between Member States and the Community institutions and bodies or between the Community institutions and bodies for purposes connected with the exercise of their respective competences.

(14) To this end measures should be adopted which are binding on the Community institutions and bodies. These measures should apply to all processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law.

(15) Where such processing is carried out by Community institutions or bodies in the exercise of activities falling outside the scope of this Regulation, in particular those laid down in Titles V and VI of the Treaty on European Union, the protection of individuals' fundamental rights and freedoms shall be ensured with due regard to Article 6 of the Treaty on European Union. Access to documents, including conditions for access to documents containing personal data, is governed by the rules adopted on the basis of Article 255 of the EC Treaty the scope of which includes Titles V and VI of the Treaty on European Union.

(16) The measures should not apply to bodies established outside the Community framework, nor should the European Data Protection Supervisor be competent to monitor the processing of personal data by such bodies.

(17) The effectiveness of the protection of individuals with regard to the processing of personal data in the Union presupposes the consistency of the relevant rules and procedures applicable to activities pertaining to different legal contexts. The development of fundamental principles on the protection of personal data in the fields of judicial cooperation in criminal affairs and police and customs cooperation, and the setting-up of a secretariat for the joint supervisory authorities established by the Europol Convention, the Convention on the Use of Information Technology for Customs Purposes and the Schengen Convention represent a first step in this regard.

(18) This Regulation should not affect the rights and obligations of Member States under Directives 95/46/EC and 97/66/EC. It is not intended to change existing procedures and practices lawfully implemented by the Member States in the field of national security, prevention of disorder or prevention, detection, investigation and prosecution of criminal offences in compliance with the Protocol on Privileges and Immunities of the European Communities and with international law.

(19) The Community institutions and bodies should inform the competent authorities in the Member States when they consider that communications on their telecommunications networks should be intercepted, in keeping with the national provisions applicable.

(20) The provisions applicable to the Community institutions and bodies should correspond to those provisions laid down in connection with the harmonisation of national laws or the implementation of other Community policies, notably in the mutual assistance sphere. It may be necessary, however, to specify and add to those provisions when it comes to ensuring protection in the case of the processing of personal data by the Community institutions and bodies.

(21) This holds true for the rights of the individuals whose data are being processed, for the obligations of the Community institutions and bodies doing the processing, and for the powers to be vested in the independent supervisory authority responsible for ensuring that this Regulation is properly applied.

(22) The rights accorded the data subject and the exercise thereof should not affect the obligations placed on the controller.

(23) The independent supervisory authority should exercise its supervisory functions in accordance with the Treaty and in compliance with human rights and fundamental freedoms. It should conduct its enquiries in compliance with the Protocol on Privileges and Immunities and with the Staff Regulations of Officials of the European Communities and the conditions of employment applicable to Other Servants of the Communities.

(24) The necessary technical measures should be adopted to allow access to the registers of processing operations carried out by Data Protection Officers through the independent supervisory authority.

(25) The decisions of the independent supervisory authority regarding exemptions, guarantees, authorisations and conditions relating to data processing operations, as defined in this Regulation, should be published in the activities report. Independently of the publication of an annual activities report, the independent supervisory authority may publish reports on specific subjects.

(26) Certain processing operations likely to present specific risks with respect to the rights and freedoms of data subjects are subject to prior checking by the independent supervisory authority. The opinion given in the context of such prior checking, including the opinion resulting from failure to reply within the set period, should be without prejudice to the subsequent exercise by the independent supervisory authority of its powers with regard to the processing operation in question.

(27) Processing of personal data for the performance of tasks carried out in the public interest by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies.

(28) In certain cases the processing of data should be authorised by Community provisions or by acts transposing Community provisions. Nevertheless, in the transitional period during which such provisions do not exist, pending their adoption, the European Data Protection Supervisor may authorise processing of such data provided that adequate safeguards are adopted. In so doing, he should take account in particular of the provisions adopted by the Member States to deal with similar cases.

(29) These cases concern the processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life which are necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law or for reasons of substantial public interest. They also concern the processing of data relating to offences, criminal convictions or security measures and authorisation to apply a decision to the data subject which produces legal effects concerning him or her or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him or her.

(30) It may be necessary to monitor the computer networks operated under the control of the Community institutions and bodies for the purposes of prevention of unauthorised use. The European Data Protection Supervisor should determine whether and under what conditions that is possible.

(31) Liability arising from any breach of this Regulation is governed by the second paragraph of Article 288 of the Treaty.

(32) In each Community institution or body one or more Data Protection Officers should ensure that the provisions of this Regulation are applied and should advise controllers on fulfilling their obligations.

(33) Under Article 21 of Council Regulation (EC) No 322/97 of 17 February 1997 on Community statistics(6), that Regulation is to apply without prejudice to Directive 95/46/EC.

(34) Under Article 8(8) of Council Regulation (EC) No 2533/98 of 23 November 1998 concerning the collection of statistical information by the European Central Bank(7), that Regulation is to apply without prejudice to Directive 95/46/EC.

(35) Under Article 1(2) of Council Regulation (Euratom, EEC) No 1588/90 of 11 June 1990 on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities(8), that Regulation does not derogate from the special Community or national provisions concerning the safeguarding of confidentiality other than statistical confidentiality.

(36) This Regulation does not aim to limit Member States' room for manoeuvre in drawing up their national laws on data protection under Article 32 of Directive 95/46/EC, in accordance with Article 249 of the Treaty,

HAVE ADOPTED THIS REGULATION:

CHAPTER I
GENERAL PROVISIONS

Article 1
Object of the Regulation

1. In accordance with this Regulation, the institutions and bodies set up by, or on the basis of, the Treaties establishing the European Communities, hereinafter referred to as "Community institutions or bodies", shall protect the funda-

mental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data and shall neither restrict nor prohibit the free flow of personal data between themselves or to recipients subject to the national law of the Member States implementing Directive 95/46/EC.

2. The independent supervisory authority established by this Regulation, hereinafter referred to as the European Data Protection Supervisor, shall monitor the application of the provisions of this Regulation to all processing operations carried out by a Community institution or body.

Article 2
Definitions

For the purposes of this Regulation:

(a) "personal data" shall mean any information relating to an identified or identifiable natural person hereinafter referred to as "data subject"; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity;

(b) "processing of personal data" hereinafter referred to as "processing" shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) "personal data filing system" hereinafter referred to as "filing system" shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(d) "controller" shall mean the Community institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by a specific Community act, the controller or the specific criteria for its nomination may be designated by such Community act;

(e) "processor" shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) "third party" shall mean a natural or legal person, public authority, agency or body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data;

(g) "recipient" shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) "the data subject's consent" shall mean any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed.

Article 3
Scope

1. This Regulation shall apply to the processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law.

2. This Regulation shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

CHAPTER II
GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

SECTION 1
PRINCIPLES RELATING TO DATA QUALITY

Article 4
Data quality

1. Personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of personal data for historical, statistical or scientific purposes shall not be considered incompatible provided that the controller provides appropriate safeguards, in particular to ensure that the data are not processed for any other purposes or used in support of measures or decisions regarding any particular individual;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. The Community institution or body shall lay down that personal data which are to be stored for longer periods for historical, statistical or scientific use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, the data shall not be used for any purpose other than for historical, statistical or scientific purposes.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION 2
CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 5
Lawfulness of processing

Personal data may be processed only if:

(a) processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed, or

(b) processing is necessary for compliance with a legal obligation to which the controller is subject, or

(c) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or

(d) the data subject has unambiguously given his or her consent, or

(e) processing is necessary in order to protect the vital interests of the data subject.

Article 6
Change of purpose

Without prejudice to Articles 4, 5 and 10:

1. Personal data shall only be processed for purposes other than those for which they have been collected if the change of purpose is expressly permitted by the internal rules of the Community institution or body.

2. Personal data collected exclusively for ensuring the security or the control of the processing systems or operations shall not be used for any other purpose, with the exception of the prevention, investigation, detection and prosecution of serious criminal offences.

Article 7
Transfer of personal data within or between Community institutions or bodies

Without prejudice to Articles 4, 5, 6 and 10:

1. Personal data shall only be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient.

2. Where the data are transferred following a request from the recipient, both the controller and the recipient shall bear the responsibility for the legitimacy of this transfer.

   The controller shall be required to verify the competence of the recipient and to make a provisional evaluation of the necessity for the transfer of the data. If doubts arise as to this necessity, the controller shall seek further information from the recipient.

The recipient shall ensure that the necessity for the transfer of the data can be subsequently verified.

3. The recipient shall process the personal data only for the purposes for which they were transmitted.

Article 8
Transfer of personal data to recipients, other than Community institutions and bodies, subject to Directive 95/46/EC

Without prejudice to Articles 4, 5, 6 and 10, personal data shall only be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC,

(a) if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, or

(b) if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced.

Article 9
Transfer of personal data to recipients, other than Community institutions and bodies, which are not subject to Directive 95/46/EC

1. Personal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out.

2. The adequacy of the level of protection afforded by the third country or international organisation in question shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the recipient third country or recipient international organisation, the rules of law, both general and sectoral, in force in the third country or international organisation in question and the professional rules and security measures which are complied with in that third country or international organisation.

3. The Community institutions and bodies shall inform the Commission and the European Data Protection Supervisor of cases where they consider the third country or international organisation in question does not ensure an adequate level of protection within the meaning of paragraph 2.

4. The Commission shall inform the Member States of any cases as referred to in paragraph 3.

5. The Community institutions and bodies shall take the necessary measures to comply with decisions taken by the Commission when it establishes, pursuant to Article 25(4) and (6) of Directive 95/46/EC, that a third country or an international organisation ensures or does not ensure an adequate level of protection.

6. By way of derogation from paragraphs 1 and 2, the Community institution or body may transfer personal data if:

   (a) the data subject has given his or her consent unambiguously to the proposed transfer; or

   (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

   (c) the transfer is necessary for the conclusion or performance of a contract entered into in the interest of the data subject between the controller and a third party; or

   (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

   (e) the transfer is necessary in order to protect the vital interests of the data subject; or

   (f) the transfer is made from a register which, according to Community law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in Community law for consultation are fulfilled in the particular case.

7. Without prejudice to paragraph 6, the European Data Protection Supervisor may authorise a transfer or a set of transfers of personal data to a third country or international organisation

which does not ensure an adequate level of protection within the meaning of paragraphs 1 and 2, where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

8. The Community institutions and bodies shall inform the European Data Protection Supervisor of categories of cases where they have applied paragraphs 6 and 7.

SECTION 3
SPECIAL CATEGORIES OF PROCESSING

Article 10
The processing of special categories of data

1. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life, are prohibited.

2. Paragraph 1 shall not apply where:

   (a) the data subject has given his or her express consent to the processing of those data, except where the internal rules of the Community institution or body provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his or her consent, or

   (b) processing is necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof, or, if necessary, insofar as it is agreed upon by the European Data Protection Supervisor, subject to adequate safeguards, or

   (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his or her consent, or

   (d) processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims, or

   (e) processing is carried out in the course of its legitimate activities with appropriate safeguards by a non-profit-seeking body which constitutes an entity integrated in a Community institution or body, not subject to national data protection law by virtue of Article 4 of Directive 95/46/EC, and with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of this body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of appropriate safeguards, and for reasons of substantial public interest, exemptions in addition to those laid down in paragraph 2 may be laid down by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by decision of the European Data Protection Supervisor.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only if authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by the European Data Protection Supervisor, subject to appropriate specific safeguards.

6. The European Data Protection Supervisor shall determine the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body.

SECTION 4
INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 11
Information to be supplied where the data have been obtained from the data subject

1. The controller shall provide a data subject from

whom data relating to himself/herself are collected with at least the following information, except where he or she already has it:

(a) the identity of the controller;

(b) the purposes of the processing operation for which the data are intended;

(c) the recipients or categories of recipients of the data;

(d) whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply;

(e) the existence of the right of access to, and the right to rectify, the data concerning him or her;

(f) any further information such as:

(i) the legal basis of the processing operation for which the data are intended,

(ii) the time-limits for storing the data,

(iii) the right to have recourse at any time to the European Data Protection Supervisor,

insofar as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

2. By way of derogation from paragraph 1, the provision of information or part of it, except for the information referred to in paragraph 1(a), (b) and (d), may be deferred as long as this is necessary for statistical purposes. The information must be provided as soon as the reason for which the information is withheld ceases to exist.

Article 12
Information to be supplied where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, the controller shall at the time of undertaking the recording of personal data or, if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed, provide the data subject with at least the following information, except where he or she already has it:

(a) the identity of the controller;

(b) the purposes of the processing operation;

(c) the categories of data concerned;

(d) the recipients or categories of recipients;

(e) the existence of the right of access to, and the right to rectify, the data concerning him or her;

(f) any further information such as:

(i) the legal basis of the processing operation for which the data are intended,

(ii) the time-limits for storing the data,

(iii) the right to have recourse at any time to the European Data Protection Supervisor,

(iv) the origin of the data, except where the controller cannot disclose this information for reasons of professional secrecy,

insofar as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by Community law. In these cases the Community institution or body shall provide for appropriate safeguards after consulting the European Data Protection Supervisor.

SECTION 5
RIGHTS OF THE DATA SUBJECT

Article 13
Right of access

The data subject shall have the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge from the controller:

(a) confirmation as to whether or not data related to him or her are being processed;

(b) information at least as to the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;

(c) communication in an intelligible form of the data undergoing processing and of any available information as to their source;

(d) knowledge of the logic involved in any automated decision process concerning him or her.

Article 14
Rectification

The data subject shall have the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data.

Article 15
Blocking

1. The data subject shall have the right to obtain from the controller the blocking of data where:

   (a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy, including the completeness, of the data, or;

   (b) the controller no longer needs them for the accomplishment of its tasks but they have to be maintained for purposes of proof, or;

   (c) the processing is unlawful and the data subject opposes their erasure and demands their blocking instead.

2. In automated filing systems blocking shall in principle be ensured by technical means. The fact that the personal data are blocked shall be indicated in the system in such a way that it becomes clear that the personal data may not be used.

3. Personal data blocked pursuant to this Article shall, with the exception of their storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of a third party.

4. The data subject who requested and obtained the blocking of his or her data shall be informed by the controller before the data are unblocked.

Article 16
Erasure

The data subject shall have the right to obtain from the controller the erasure of data if their processing is unlawful, particularly where the provisions of Sections 1, 2 and 3 of Chapter II have been infringed.

Article 17
Notification to third parties

The data subject shall have the right to obtain from the controller the notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking pursuant to Articles 13 to 16 unless this proves impossible or involves a disproportionate effort.

Article 18
The data subject's right to object

The data subject shall have the right:

(a) to object at any time, on compelling legitimate grounds relating to his or her particular situation, to the processing of data relating to him or her, except in the cases covered by Article 5(b), (c) and (d). Where there is a justified objection, the processing in question may no longer involve those data;

(b) to be informed before personal data are disclosed for the first time to third parties or before they are used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosure or use.

Article 19
Automated individual decisions

The data subject shall have the right not to be subject to a decision which produces legal effects concerning him or her or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him or her, such as his or her performance at work, reliability or conduct, unless the decision is expressly authorised pursuant to national or Community legislation or, if necessary, by the European Data Protection Supervisor. In either case, measures to safeguard the data subject's legitimate interests, such as arrangements allowing him or her to put his or her point of view, must be taken.

SECTION 6
EXEMPTIONS AND RESTRICTIONS

Article 20
Exemptions and restrictions

1. The Community institutions and bodies may restrict the application of Article 4(1), Article 11, Article 12(1), Articles 13 to 17 and Article 37(1) where such restriction constitutes a necessary measure to safeguard:

   (a) the prevention, investigation, detection and prosecution of criminal offences;

(b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters;

(c) the protection of the data subject or of the rights and freedoms of others;

(d) the national security, public security or defence of the Member States;

(e) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the cases referred to in (a) and (b).

2. Articles 13 to 16 shall not apply when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of compiling statistics, provided that there is clearly no risk of breaching the privacy of the data subject and that the controller provides adequate legal safeguards, in particular to ensure that the data are not used for taking measures or decisions regarding particular individuals.

3. If a restriction provided for by paragraph 1 is imposed, the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Supervisor.

4. If a restriction provided for by paragraph 1 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.

5. Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect.

SECTION 7
CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 21
Confidentiality of processing

A person employed with a Community institution or body and any Community institution or body itself acting as processor, with access to personal data, shall not process them except on instructions from the controller, unless required to do so by national or Community law.

Article 22
Security of processing

1. Having regard to the state of the art and the cost of their implementation, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected.

   Such measures shall be taken in particular to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing.

2. Where personal data are processed by automated means, measures shall be taken as appropriate in view of the risks in particular with the aim of:

   (a) preventing any unauthorised person from gaining access to computer systems processing personal data;

   (b) preventing any unauthorised reading, copying, alteration or removal of storage media;

   (c) preventing any unauthorised memory inputs as well as any unauthorised disclosure, alteration or erasure of stored personal data;

   (d) preventing unauthorised persons from using data-processing systems by means of data transmission facilities;

   (e) ensuring that authorised users of a data-processing system can access no personal data other than those to which their access right refers;

   (f) recording which personal data have been communicated, at what times and to whom;

   (g) ensuring that it will subsequently be possible to check which personal data have been processed, at what times and by whom;

   (h) ensuring that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the contracting institution or body;

   (i) ensuring that, during communication of personal data and during transport of stor-

age media, the data cannot be read, copied or erased without authorisation;

(j) designing the organisational structure within an institution or body in such a way that it will meet the special requirements of data protection.

Article 23
Processing of personal data on behalf of controllers

1. Where a processing operation is carried out on its behalf, the controller shall choose a processor providing sufficient guarantees in respect of the technical and organisational security measures required by Article 22 and ensure compliance with those measures.

2. The carrying out of a processing operation by way of a processor shall be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

   (a) the processor shall act only on instructions from the controller;

   (b) the obligations set out in Articles 21 and 22 shall also be incumbent on the processor unless, by virtue of Article 16 or Article 17(3), second indent, of Directive 95/46/EC, the processor is already subject to obligations with regard to confidentiality and security laid down in the national law of one of the Member States.

3. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in Article 22 shall be in writing or in another equivalent form.

SECTION 8
DATA PROTECTION OFFICER

Article 24
Appointment and tasks of the Data Protection Officer

1. Each Community institution and Community body shall appoint at least one person as data protection officer. That person shall have the task of:

   (a) ensuring that controllers and data subjects are informed of their rights and obligations pursuant to this Regulation;

   (b) responding to requests from the European Data Protection Supervisor and, within the sphere of his or her competence, cooperating with the European Data Protection Supervisor at the latter's request or on his or her own initiative;

   (c) ensuring in an independent manner the internal application of the provisions of this Regulation;

   (d) keeping a register of the processing operations carried out by the controller, containing the items of information referred to in Article 25(2);

   (e) notifying the European Data Protection Supervisor of the processing operations likely to present specific risks within the meaning of Article 27.

   That person shall thus ensure that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

2. The Data Protection Officer shall be selected on the basis of his or her personal and professional qualities and, in particular, his or her expert knowledge of data protection.

3. The selection of the Data Protection Officer shall not be liable to result in a conflict of interests between his or her duty as Data Protection Officer and any other official duties, in particular in relation to the application of the provisions of this Regulation.

4. The Data Protection Officer shall be appointed for a term of between two and five years. He or she shall be eligible for reappointment up to a maximum total term of ten years. He or she may be dismissed from the post of Data Protection Officer by the Community institution or body which appointed him or her only with the consent of the European Data Protection Supervisor, if he or she no longer fulfils the conditions required for the performance of his or her duties.

5. After his or her appointment the Data Protection Officer shall be registered with the European Data Protection Supervisor by the institution or body which appointed him or her.

6. The Community institution or body which appointed the Data Protection Officer shall provide him or her with the staff and resources necessary to carry out his or her duties.

7. With respect to the performance of his or her duties, the Data Protection Officer may not receive any instructions.

8. Further implementing rules concerning the Data Protection Officer shall be adopted by each Community institution or body in accordance with the provisions in the Annex. The implementing rules shall in particular concern the tasks, duties and powers of the Data Protection Officer.

Article 25
Notification to the Data Protection Officer

1. The controller shall give prior notice to the Data Protection Officer of any processing operation or set of such operations intended to serve a single purpose or several related purposes.
2. The information to be given shall include:
   (a) the name and address of the controller and an indication of the organisational parts of an institution or body entrusted with the processing of personal data for a particular purpose;
   (b) the purpose or purposes of the processing;
   (c) a description of the category or categories of data subjects and of the data or categories of data relating to them;
   (d) the legal basis of the processing operation for which the data are intended;
   (e) the recipients or categories of recipient to whom the data might be disclosed;
   (f) a general indication of the time limits for blocking and erasure of the different categories of data;
   (g) proposed transfers of data to third countries or international organisations;
   (h) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 22 to ensure security of processing.
3. Any change affecting information referred to in paragraph 2 shall be notified promptly to the Data Protection Officer.

Article 26
Register

A register of processing operations notified in accordance with Article 25 shall be kept by each Data Protection Officer.

The registers shall contain at least the information referred to in Article 25(2)(a) to (g). The registers may be inspected by any person directly or indirectly through the European Data Processing Supervisor.

SECTION 9
PRIOR CHECKING BY THE EUROPEAN DATA PROTECTION SUPERVISOR AND OBLIGATION TO COOPERATE

Article 27
Prior checking

1. Processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes shall be subject to prior checking by the European Data Protection Supervisor.
2. The following processing operations are likely to present such risks:
   (a) processing of data relating to health and to suspected offences, offences, criminal convictions or security measures;
   (b) processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct;
   (c) processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes;
   (d) processing operations for the purpose of excluding individuals from a right, benefit or contract.
3. The prior checks shall be carried out by the European Data Protection Supervisor following receipt of a notification from the Data Protection Officer who, in case of doubt as to the need for prior checking, shall consult the European Data Protection Supervisor.
4. The European Data Protection Supervisor shall deliver his or her opinion within two months following receipt of the notification. This period may be suspended until the European Data Protection Supervisor has obtained any further information that he or she may have requested. When the complexity of the matter so requires, this period may also be extended for a further two months, by decision of the European Data Protection Supervisor. This decision shall be notified to the controller prior to expiry of the initial two-month period.

   If the opinion has not been delivered by the

end of the two-month period, or any extension thereof, it shall be deemed to be favourable.

If the opinion of the European Data Protection Supervisor is that the notified processing may involve a breach of any provision of this Regulation, he or she shall where appropriate make proposals to avoid such breach. Where the controller does not modify the processing operation accordingly, the European Data Protection Supervisor may exercise the powers granted to him or her under Article 47(1).

5. The European Data Protection Supervisor shall keep a register of all processing operations that have been notified to him or her pursuant to paragraph 2. The register shall contain the information referred to in Article 25 and shall be open to public inspection.

Article 28
Consultation

1. The Community institutions and bodies shall inform the European Data Protection Supervisor when drawing up administrative measures relating to the processing of personal data involving a Community institution or body alone or jointly with others.

2. When it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission shall consult the European Data Protection Supervisor.

Article 29
Obligation to provide information

The Community institutions and bodies shall inform the European Data Protection Supervisor of the measures taken further to his or her decisions or authorisations as referred to in Article 46(h).

Article 30
Obligation to cooperate

At his or her request, controllers shall assist the European Data Protection Supervisor in the performance of his or her duties, in particular by providing the information referred to in Article 47(2)(a) and by granting access as provided in Article 47(2)(b).

Article 31
Obligation to react to allegations

In response to the European Data Protection Supervisor's exercise of his or her powers under Article 47(1)(b), the controller concerned shall inform the Supervisor of its views within a reasonable period to be specified by the Supervisor. The reply shall also include a description of the measures taken, if any, in response to the remarks of the European Data Protection Supervisor.

CHAPTER III
REMEDIES

Article 32
Remedies

1. The Court of Justice of the European Communities shall have jurisdiction to hear all disputes which relate to the provisions of this Regulation, including claims for damages.

2. Without prejudice to any judicial remedy, every data subject may lodge a complaint with the European Data Protection Supervisor if he or she considers that his or her rights under Article 286 of the Treaty have been infringed as a result of the processing of his or her personal data by a Community institution or body.

   In the absence of a response by the European Data Protection Supervisor within six months, the complaint shall be deemed to have been rejected.

3. Actions against decisions of the European Data Protection Supervisor shall be brought before the Court of Justice of the European Communities.

4. Any person who has suffered damage because of an unlawful processing operation or any action incompatible with this Regulation shall have the right to have the damage made good in accordance with Article 288 of the Treaty.

Article 33
Complaints by Community staff

Any person employed with a Community institution or body may lodge a complaint with the European Data Protection Supervisor regarding an alleged breach of the provisions of this Regulation governing the processing of personal data, without acting through official channels. No-one shall suffer prejudice on account of a complaint lodged with the European Data Protection Supervisor alleging a breach of the provisions governing the processing of personal data.

CHAPTER IV
PROTECTION OF PERSONAL DATA AND PRIVACY IN THE CONTEXT OF INTERNAL TELECOMMUNICATIONS NETWORKS

Article 34
Scope

Without prejudice to the other provisions of this Regulation, this Chapter shall apply to the processing of personal data in connection with the use of telecommunications networks or terminal equipment operated under the control of a Community institution or body.

For the purposes of this Chapter, "user" shall mean any natural person using a telecommunications network or terminal equipment operated under the control of a Community institution or body.

Article 35
Security

1. The Community institutions and bodies shall take appropriate technical and organisational measures to safeguard the secure use of the telecommunications networks and terminal equipment, if necessary in conjunction with the providers of publicly available telecommunications services or the providers of public telecommunications networks. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.
2. In the event of any particular risk of a breach of the security of the network and terminal equipment, the Community institution or body concerned shall inform users of the existence of that risk and of any possible remedies and alternative means of communication.

Article 36
Confidentiality of communications

Community institutions and bodies shall ensure the confidentiality of communications by means of telecommunications networks and terminal equipment, in accordance with the general principles of Community law.

Article 37
Traffic and billing data

1. Without prejudice to the provisions of paragraphs 2, 3 and 4, traffic data relating to users which are processed and stored to establish calls and other connections over the telecommunications network shall be erased or made anonymous upon termination of the call or other connection.
2. If necessary, traffic data as indicated in a list agreed by the European Data Protection Supervisor may be processed for the purpose of telecommunications budget and traffic management, including the verification of authorised use of the telecommunications systems. These data shall be erased or made anonymous as soon as possible and no later than six months after collection, unless they need to be kept for a longer period to establish, exercise or defend a right in a legal claim pending before a court.
3. Processing of traffic and billing data shall only be carried out by persons handling billing, traffic or budget management.
4. Users of the telecommunication networks shall have the right to receive non-itemised bills or other records of calls made.

Article 38
Directories of users

1. Personal data contained in printed or electronic directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.
2. The Community institutions and bodies shall take all the necessary measures to prevent personal data contained in those directories, regardless of whether they are accessible to the public or not, from being used for direct marketing purposes.

Article 39
Presentation and restriction of calling and connected line identification

1. Where presentation of calling-line identification is offered, the calling user shall have the possibility via a simple means, free of charge, to eliminate the presentation of the calling-line identification.
2. Where presentation of calling-line identification is offered, the called user shall have the possibility via a simple means, free of charge, to prevent

the presentation of the calling-line identification of incoming calls.

3. Where presentation of connected-line identification is offered, the called user shall have the possibility via a simple means, free of charge, to eliminate the presentation of the connected-line identification to the calling user.

4. Where presentation of calling or connected-line identification is offered, the Community institutions and bodies shall inform the users thereof and of the possibilities set out in paragraphs 1, 2 and 3.

Article 40
Derogations

Community institutions and bodies shall ensure that there are transparent procedures governing the way in which they may override the elimination of the presentation of calling-line identification:

(a) on a temporary basis, upon application of a user requesting the tracing of malicious or nuisance calls;

(b) on a per-line basis for organisational entities dealing with emergency calls, for the purpose of answering such calls.

CHAPTER V INDEPENDENT SUPERVISORY AUTHORITY: THE EUROPEAN DATA PROTECTION SUPERVISOR

Article 41
European Data Protection Supervisor

1. An independent supervisory authority is hereby established referred to as the European Data Protection Supervisor.

2. With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies.

   The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and any other Community act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body, and for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data. To these ends he or she shall fulfil the duties provided for in Article 46 and exercise the powers granted in Article 47.

Article 42
Appointment

1. The European Parliament and the Council shall appoint by common accord the European Data Protection Supervisor for a term of five years, on the basis of a list drawn up by the Commission following a public call for candidates. An Assistant Supervisor shall be appointed in accordance with the same procedure and for the same term, who shall assist the Supervisor in all the latter's duties and act as a replacement when the Supervisor is absent or prevented from attending to them.

2. The European Data Protection Supervisor shall be chosen from persons whose independence is beyond doubt and who are acknowledged as having the experience and skills required to perform the duties of European Data Protection Supervisor, for example because they belong or have belonged to the supervisory authorities referred to in Article 28 of Directive 95/46/EC.

3. The European Data Protection Supervisor shall be eligible for reappointment.

4. Apart from normal replacement or death, the duties of the European Data Protection Supervisor shall end in the event of resignation or compulsory retirement in accordance with paragraph 5.

5. The European Data Protection Supervisor may be dismissed or deprived of his or her right to a pension or other benefits in its stead by the Court of Justice at the request of the European Parliament, the Council or the Commission, if he or she no longer fulfils the conditions required for the performance of his or her duties or if he or she is guilty of serious misconduct.

6. In the event of normal replacement or voluntary resignation, the European Data Protection Supervisor shall nevertheless remain in office until he or she has been replaced.

7. Articles 12 to 15 and 18 of the Protocol on the Privileges and Immunities of the European Communities shall also apply to the European

Data Protection Supervisor.

8. Paragraphs 2 to 7 shall apply to the Assistant Supervisor.

Article 43
Regulations and general conditions governing the performance of the European Data Protection Supervisor's duties, staff and financial resources

1. The European Parliament, the Council and the Commission shall by common accord determine the regulations and general conditions governing the performance of the European Data Protection Supervisor's duties and in particular his or her salary, allowances and any other benefits in lieu of remuneration.
2. The budget authority shall ensure that the European Data Protection Supervisor is provided with the human and financial resources necessary for the performance of his or her tasks.
3. The European Data Protection Supervisor's budget shall be shown in a separate budget heading in Section VIII of the general budget of the European Union.
4. The European Data Protection Supervisor shall be assisted by a Secretariat. The officials and the other staff members of the Secretariat shall be appointed by the European Data Protection Supervisor; their superior shall be the European Data Protection Supervisor and they shall be subject exclusively to his or her direction. Their numbers shall be decided each year as part of the budgetary procedure.
5. The officials and the other staff members of the European Data Protection Supervisor's Secretariat shall be subject to the rules and regulations applicable to officials and other servants of the European Communities.
6. In matters concerning the Secretariat staff, the European Data Protection Supervisor shall have the same status as the institutions within the meaning of Article 1 of the Staff Regulations of Officials of the European Communities.

Article 44
Independence

1. The European Data Protection Supervisor shall act in complete independence in the performance of his or her duties.
2. The European Data Protection Supervisor shall, in the performance of his or her duties, neither seek nor take instructions from anybody.
3. The European Data Protection Supervisor shall refrain from any action incompatible with his or her duties and shall not, during his or her term of office, engage in any other occupation, whether gainful or not.
4. The European Data Protection Supervisor shall, after his or her term of office, behave with integrity and discretion as regards the acceptance of appointments and benefits.

Article 45
Professional secrecy

The European Data Protection Supervisor and his or her staff shall, both during and after their term of office, be subject to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.

Article 46
Duties

The European Data Protection Supervisor shall:

(a) hear and investigate complaints, and inform the data subject of the outcome within a reasonable period;

(b) conduct inquiries either on his or her own initiative or on the basis of a complaint, and inform the data subjects of the outcome within a reasonable period;

(c) monitor and ensure the application of the provisions of this Regulation and any other Community act relating to the protection of natural persons with regard to the processing of personal data by a Community institution or body with the exception of the Court of Justice of the European Communities acting in its judicial capacity;

(d) advise all Community institutions and bodies, either on his or her own initiative or in response to a consultation, on all matters concerning the processing of personal data, in particular before they draw up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of personal data;

(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;

(f)

(i) cooperate with the national supervisory authorities referred to in Article 28 of Directive 95/46/EC in the countries to which that Directive applies to the extent necessary for the performance of their respective duties, in particular by exchanging all useful information, requesting such authority or body to exercise its powers or responding to a request from such authority or body;

(ii) also cooperate with the supervisory data protection bodies established under Title VI of the Treaty on European Union particularly with a view to improving consistency in applying the rules and procedures with which they are respectively responsible for ensuring compliance;

(g) participate in the activities of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up by Article 29 of Directive 95/46/EC;

(h) determine, give reasons for and make public the exemptions, safeguards, authorisations and conditions mentioned in Article 10(2)(b),(4), (5) and (6), in Article 12(2), in Article 19 and in Article 37(2);

(i) keep a register of processing operations notified to him or her by virtue of Article 27(2) and registered in accordance with Article 27(5), and provide means of access to the registers kept by the Data Protection Officers under Article 26;

(j) carry out a prior check of processing notified to him or her;

(k) establish his or her Rules of Procedure.

Article 47
Powers

1. The European Data Protection Supervisor may:

(a) give advice to data subjects in the exercise of their rights;

(b) refer the matter to the controller in the event of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects;

(c) order that requests to exercise certain rights in relation to data be complied with where such requests have been refused in breach of Articles 13 to 19;

(d) warn or admonish the controller;

(e) order the rectification, blocking, erasure or destruction of all data when they have been processed in breach of the provisions governing the processing of personal data and the notification of such actions to third parties to whom the data have been disclosed;

(f) impose a temporary or definitive ban on processing;

(g) refer the matter to the Community institution or body concerned and, if necessary, to the European Parliament, the Council and the Commission;

(h) refer the matter to the Court of Justice of the European Communities under the conditions provided for in the Treaty;

(i) intervene in actions brought before the Court of Justice of the European Communities.

2. The European Data Protection Supervisor shall have the power:

(a) to obtain from a controller or Community institution or body access to all personal data and to all information necessary for his or her enquiries;

(b) to obtain access to any premises in which a controller or Community institution or body carries on its activities when there are reasonable grounds for presuming that an activity covered by this Regulation is being carried out there.

Article 48
Activities report

1. The European Data Protection Supervisor shall submit an annual report on his or her activities to the European Parliament, the Council and the Commission and at the same time make it public.

2. The European Data Protection Supervisor shall forward the activities report to the other Community institutions and bodies, which may submit comments with a view to possible examination of the report in the European Parliament, in particular in relation to the description of the measures taken in response to the remarks made by the European Data Protection Supervisor under Article 31.

CHAPTER VI
FINAL PROVISIONS

Article 49
Sanctions

Any failure to comply with the obligations pursuant to this Regulation, whether intentionally or through negligence on his or her part, shall make an official or other servant of the European Communities liable to disciplinary action, in accordance with the rules and procedures laid down in the Staff Regulations of Officials of the European Communities or in the conditions of employment applicable to other servants.

Article 50
Transitional period

Community institutions and bodies shall ensure that processing operations already under way on the date this Regulation enters into force are brought into conformity with this Regulation within one year of that date.

Article 51
Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Communities.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 18 December 2000.
For the European Parliament
The President N. Fontaine
For the Council
The President D. Voynet

[1] OJ C 376E, 28.12.1999, p. 24.

[2] OJ C 51, 23.2.2000, p. 48.

[3] Opinion of the European Parliament of 14 November 2000 and Council Decision of 30 November 2000.

[4] OJ L 281, 23.11.1995, p. 31.

[5] OJ L 24, 30.1.1998, p. 1.

[6] OJ L 52, 22.2.1997, p. 1.

[7] OJ L 318, 27.11.1998, p. 8.

[8] OJ L 151, 15. 6.1990, p. 1. Regulation as amended by Regulation (EC) No 322/97 (OJ L 52, 22.2.1997, p. 1).

ANNEX

1. The Data Protection Officer may make recommendations for the practical improvement of data protection to the Community institution or body which appointed him or her and advise it and the controller concerned on matters concerning the application of data protection provisions. Furthermore he or she may, on his or her own initiative or at the request of the Community institution or body which appointed him or her, the controller, the Staff Committee concerned or any individual, investigate matters and occurrences directly relating to his or her tasks and which come to his or her notice, and report back to the person who commissioned the investigation or to the controller.
2. The Data Protection Officer may be consulted by the Community institution or body which appointed him or her, by the controller concerned, by the Staff Committee concerned and by any individual, without going through the official channels, on any matter concerning the interpretation or application of this Regulation.
3. No one shall suffer prejudice on account of a matter brought to the attention of the competent Data Protection Officer alleging that a breach of the provisions of this Regulation has taken place.
4. Every controller concerned shall be required to assist the Data Protection Officer in performing his or her duties and to give information in reply to questions. In performing his or her duties, the Data Protection Officer shall have access at all times to the data forming the subject-matter of processing operations and to all offices, data-processing installations and data carriers.
5. To the extent required, the Data Protection Officer shall be relieved of other activities. The Data Protection Officer and his or her staff, to whom Article 287 of the Treaty shall apply, shall be required not to divulge information or documents which they obtain in the course of their duties.

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof,

Having regard to the proposal from the Commission(1),

Having regard to the opinion of the Economic and Social Committee(2),

Acting in accordance with the procedure laid down in Article 251 of the Treaty(3),

Whereas:

(1) The Treaty provides for the establishment of an internal market and the institution of a system ensuring that competition in the internal market is not distorted. Harmonisation of the laws of the Member States on copyright and related rights contributes to the achievement of these objectives.

(2) The European Council, meeting at Corfu on 24 and 25 June 1994, stressed the need to create a general and flexible legal framework at Community level in order to foster the development of the information society in Europe. This requires, inter alia, the existence of an internal market for new products and services. Important Community legislation to ensure such a regulatory framework is already in place or its adoption is well under way. Copyright and related rights play an important role in this context as they protect and stimulate the development and marketing of new products and services and the creation and exploitation of their creative content.

(3) The proposed harmonisation will help to implement the four freedoms of the internal market and relates to compliance with the fundamental principles of law and especially of property, including intellectual property, and freedom of expression and the public interest.

(4) A harmonised legal framework on copyright and related rights, through increased legal certainty and while providing for a high level of protection of intellectual property, will foster substantial investment in creativity and innovation, including network infrastructure, and lead in turn to growth and increased competitiveness of European industry, both in the area of content provision and information technology and more generally across a wide range of industrial and cultural sectors. This will safeguard employment and encourage new job creation.

(5) Technological development has multiplied and diversified the vectors for creation, production and exploitation. While no new concepts for the protection of intellectual property are needed, the current law on copyright and related rights should be adapted and supplemented to respond adequately to economic realities such as new forms of exploitation.

(6) Without harmonisation at Community level, legislative activities at national level which have already been initiated in a number of Member States in order to respond to the technological challenges might result in significant differences in protection and thereby in restrictions on the free movement of services and products incorporating, or based on, intellectual property, leading to a refragmentation of the internal market and legislative inconsistency. The impact of such legislative differences and uncertainties will become more significant with the further development of the information society, which has already greatly increased transborder exploitation of intellectual property. This development will and should further increase. Significant legal differences and uncertainties in protection may hinder economies of scale for new products and services containing copyright and related rights.

(7) The Community legal framework for the protection of copyright and related rights must, therefore, also be adapted and supplemented as far as is necessary for the smooth functioning of the internal market. To that end, those national provisions on copyright and related rights which vary considerably from one Member State to another or which cause legal uncertainties hindering the smooth functioning of the internal market and the proper development

of the information society in Europe should be adjusted, and inconsistent national responses to the technological developments should be avoided, whilst differences not adversely affecting the functioning of the internal market need not be removed or prevented.

(8) The various social, societal and cultural implications of the information society require that account be taken of the specific features of the content of products and services.

(9) Any harmonisation of copyright and related rights must take as a basis a high level of protection, since such rights are crucial to intellectual creation. Their protection helps to ensure the maintenance and development of creativity in the interests of authors, performers, producers, consumers, culture, industry and the public at large. Intellectual property has therefore been recognised as an integral part of property.

(10) If authors or performers are to continue their creative and artistic work, they have to receive an appropriate reward for the use of their work, as must producers in order to be able to finance this work. The investment required to produce products such as phonograms, films or multimedia products, and services such as "on-demand" services, is considerable. Adequate legal protection of intellectual property rights is necessary in order to guarantee the availability of such a reward and provide the opportunity for satisfactory returns on this investment.

(11) A rigorous, effective system for the protection of copyright and related rights is one of the main ways of ensuring that European cultural creativity and production receive the necessary resources and of safeguarding the independence and dignity of artistic creators and performers.

(12) Adequate protection of copyright works and subject-matter of related rights is also of great importance from a cultural standpoint. Article 151 of the Treaty requires the Community to take cultural aspects into account in its action.

(13) A common search for, and consistent application at European level of, technical measures to protect works and other subject-matter and to provide the necessary information on rights are essential insofar as the ultimate aim of these measures is to give effect to the principles and guarantees laid down in law.

(14) This Directive should seek to promote learning and culture by protecting works and other subject-matter while permitting exceptions or limitations in the public interest for the purpose of education and teaching.

(15) The Diplomatic Conference held under the auspices of the World Intellectual Property Organisation (WIPO) in December 1996 led to the adoption of two new Treaties, the "WIPO Copyright Treaty" and the "WIPO Performances and Phonograms Treaty", dealing respectively with the protection of authors and the protection of performers and phonogram producers. Those Treaties update the international protection for copyright and related rights significantly, not least with regard to the so-called "digital agenda", and improve the means to fight piracy world-wide. The Community and a majority of Member States have already signed the Treaties and the process of making arrangements for the ratification of the Treaties by the Community and the Member States is under way. This Directive also serves to implement a number of the new international obligations.

(16) Liability for activities in the network environment concerns not only copyright and related rights but also other areas, such as defamation, misleading advertising, or infringement of trademarks, and is addressed horizontally in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ("Directive on electronic commerce") (4), which clarifies and harmonises various legal issues relating to information society services including electronic commerce. This Directive should be implemented within a timescale similar to that for the implementation of the Directive on electronic commerce, since that Directive provides a harmonised framework of principles and provisions relevant inter alia to important parts of this Directive. This Directive is without prejudice to provisions relating to liability in that Directive.

(17) It is necessary, especially in the light of the requirements arising out of the digital environment, to ensure that collecting societies achieve a higher level of rationalisation and transparency with regard to compliance with competition rules.

(18) This Directive is without prejudice to the arrangements in the Member States concerning the management of rights such as extended collective licences.

(19) The moral rights of rightholders should be exercised according to the legislation of the Mem-

ber States and the provisions of the Berne Convention for the Protection of Literary and Artistic Works, of the WIPO Copyright Treaty and of the WIPO Performances and Phonograms Treaty. Such moral rights remain outside the scope of this Directive.

(20) This Directive is based on principles and rules already laid down in the Directives currently in force in this area, in particular Directives 91/250/EEC(5), 92/100/EEC(6), 93/83/EEC(7), 93/98/EEC(8) and 96/9/EC(9), and it develops those principles and rules and places them in the context of the information society. The provisions of this Directive should be without prejudice to the provisions of those Directives, unless otherwise provided in this Directive.

(21) This Directive should define the scope of the acts covered by the reproduction right with regard to the different beneficiaries. This should be done in conformity with the acquis communautaire. A broad definition of these acts is needed to ensure legal certainty within the internal market.

(22) The objective of proper support for the dissemination of culture must not be achieved by sacrificing strict protection of rights or by tolerating illegal forms of distribution of counterfeited or pirated works.

(23) This Directive should harmonise further the author's right of communication to the public. This right should be understood in a broad sense covering all communication to the public not present at the place where the communication originates. This right should cover any such transmission or retransmission of a work to the public by wire or wireless means, including broadcasting. This right should not cover any other acts.

(24) The right to make available to the public subject-matter referred to in Article 3(2) should be understood as covering all acts of making available such subject-matter to members of the public not present at the place where the act of making available originates, and as not covering any other acts.

(25) The legal uncertainty regarding the nature and the level of protection of acts of on-demand transmission of copyright works and subject-matter protected by related rights over networks should be overcome by providing for harmonised protection at Community level. It should be made clear that all rightholders recognised by this Directive should have an exclusive right to make available to the public copyright works or any other subject-matter by way of interactive on-demand transmissions. Such interactive on-demand transmissions are characterised by the fact that members of the public may access them from a place and at a time individually chosen by them.

(26) With regard to the making available in on-demand services by broadcasters of their radio or television productions incorporating music from commercial phonograms as an integral part thereof, collective licensing arrangements are to be encouraged in order to facilitate the clearance of the rights concerned.

(27) The mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Directive.

(28) Copyright protection under this Directive includes the exclusive right to control distribution of the work incorporated in a tangible article. The first sale in the Community of the original of a work or copies thereof by the rightholder or with his consent exhausts the right to control resale of that object in the Community. This right should not be exhausted in respect of the original or of copies thereof sold by the rightholder or with his consent outside the Community. Rental and lending rights for authors have been established in Directive 92/100/EEC. The distribution right provided for in this Directive is without prejudice to the provisions relating to the rental and lending rights contained in Chapter I of that Directive.

(29) The question of exhaustion does not arise in the case of services and on-line services in particular. This also applies with regard to a material copy of a work or other subject-matter made by a user of such a service with the consent of the rightholder. Therefore, the same applies to rental and lending of the original and copies of works or other subject-matter which are services by nature. Unlike CD-ROM or CD-I, where the intellectual property is incorporated in a material medium, namely an item of goods, every on-line service is in fact an act which should be subject to authorisation where the copyright or related right so provides.

(30) The rights referred to in this Directive may be transferred, assigned or subject to the granting of contractual licences, without prejudice to the relevant national legislation on copyright and related rights.

(31) A fair balance of rights and interests between the different categories of rightholders, as well as between the different categories of rightholders and users of protected subject-matter must be safeguarded. The existing exceptions and limitations to the rights as set out by the Member States have to be reassessed in the light of the new electronic environment. Existing differences in the exceptions and limitations to certain restricted acts have direct negative effects on the functioning of the internal market of copyright and related rights. Such differences could well become more pronounced in view of the further development of transborder exploitation of works and cross-border activities. In order to ensure the proper functioning of the internal market, such exceptions and limitations should be defined more harmoniously. The degree of their harmonisation should be based on their impact on the smooth functioning of the internal market.

(32) This Directive provides for an exhaustive enumeration of exceptions and limitations to the reproduction right and the right of communication to the public. Some exceptions or limitations only apply to the reproduction right, where appropriate. This list takes due account of the different legal traditions in Member States, while, at the same time, aiming to ensure a functioning internal market. Member States should arrive at a coherent application of these exceptions and limitations, which will be assessed when reviewing implementing legislation in the future.

(33) The exclusive right of reproduction should be subject to an exception to allow certain acts of temporary reproduction, which are transient or incidental reproductions, forming an integral and essential part of a technological process and carried out for the sole purpose of enabling either efficient transmission in a network between third parties by an intermediary, or a lawful use of a work or other subject-matter to be made. The acts of reproduction concerned should have no separate economic value on their own. To the extent that they meet these conditions, this exception should include acts which enable browsing as well as acts of caching to take place, including those which enable transmission systems to function efficiently, provided that the intermediary does not modify the information and does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information. A use should be considered lawful where it is authorised by the rightholder or not restricted by law.

(34) Member States should be given the option of providing for certain exceptions or limitations for cases such as educational and scientific purposes, for the benefit of public institutions such as libraries and archives, for purposes of news reporting, for quotations, for use by people with disabilities, for public security uses and for uses in administrative and judicial proceedings.

(35) In certain cases of exceptions or limitations, rightholders should receive fair compensation to compensate them adequately for the use made of their protected works or other subject-matter. When determining the form, detailed arrangements and possible level of such fair compensation, account should be taken of the particular circumstances of each case. When evaluating these circumstances, a valuable criterion would be the possible harm to the rightholders resulting from the act in question. In cases where rightholders have already received payment in some other form, for instance as part of a licence fee, no specific or separate payment may be due. The level of fair compensation should take full account of the degree of use of technological protection measures referred to in this Directive. In certain situations where the prejudice to the rightholder would be minimal, no obligation for payment may arise.

(36) The Member States may provide for fair compensation for rightholders also when applying the optional provisions on exceptions or limitations which do not require such compensation.

(37) Existing national schemes on reprography, where they exist, do not create major barriers to the internal market. Member States should be allowed to provide for an exception or limitation in respect of reprography.

(38) Member States should be allowed to provide for an exception or limitation to the reproduction right for certain types of reproduction of audio, visual and audio-visual material for private use, accompanied by fair compensation. This may include the introduction or continuation of remuneration schemes to compensate for the prejudice to rightholders. Although differences between those remuneration schemes affect the functioning of the internal market, those differences, with respect to analogue private reproduction, should not have a significant impact on the development of the information society. Digital private copying is likely to be more widespread and have a greater economic im-

pact. Due account should therefore be taken of the differences between digital and analogue private copying and a distinction should be made in certain respects between them.

(39) When applying the exception or limitation on private copying, Member States should take due account of technological and economic developments, in particular with respect to digital private copying and remuneration schemes, when effective technological protection measures are available. Such exceptions or limitations should not inhibit the use of technological measures or their enforcement against circumvention.

(40) Member States may provide for an exception or limitation for the benefit of certain non-profit making establishments, such as publicly accessible libraries and equivalent institutions, as well as archives. However, this should be limited to certain special cases covered by the reproduction right. Such an exception or limitation should not cover uses made in the context of on-line delivery of protected works or other subject-matter. This Directive should be without prejudice to the Member States' option to derogate from the exclusive public lending right in accordance with Article 5 of Directive 92/100/EEC. Therefore, specific contracts or licences should be promoted which, without creating imbalances, favour such establishments and the disseminative purposes they serve.

(41) When applying the exception or limitation in respect of ephemeral recordings made by broadcasting organisations it is understood that a broadcaster's own facilities include those of a person acting on behalf of and under the responsibility of the broadcasting organisation.

(42) When applying the exception or limitation for non-commercial educational and scientific research purposes, including distance learning, the non-commercial nature of the activity in question should be determined by that activity as such. The organisational structure and the means of funding of the establishment concerned are not the decisive factors in this respect.

(43) It is in any case important for the Member States to adopt all necessary measures to facilitate access to works by persons suffering from a disability which constitutes an obstacle to the use of the works themselves, and to pay particular attention to accessible formats.

(44) When applying the exceptions and limitations provided for in this Directive, they should be exercised in accordance with international obligations. Such exceptions and limitations may not be applied in a way which prejudices the legitimate interests of the rightholder or which conflicts with the normal exploitation of his work or other subject-matter. The provision of such exceptions or limitations by Member States should, in particular, duly reflect the increased economic impact that such exceptions or limitations may have in the context of the new electronic environment. Therefore, the scope of certain exceptions or limitations may have to be even more limited when it comes to certain new uses of copyright works and other subject-matter.

(45) The exceptions and limitations referred to in Article 5(2), (3) and (4) should not, however, prevent the definition of contractual relations designed to ensure fair compensation for the rightholders insofar as permitted by national law.

(46) Recourse to mediation could help users and rightholders to settle disputes. The Commission, in cooperation with the Member States within the Contact Committee, should undertake a study to consider new legal ways of settling disputes concerning copyright and related rights.

(47) Technological development will allow rightholders to make use of technological measures designed to prevent or restrict acts not authorised by the rightholders of any copyright, rights related to copyright or the sui generis right in databases. The danger, however, exists that illegal activities might be carried out in order to enable or facilitate the circumvention of the technical protection provided by these measures. In order to avoid fragmented legal approaches that could potentially hinder the functioning of the internal market, there is a need to provide for harmonised legal protection against circumvention of effective technological measures and against provision of devices and products or services to this effect.

(48) Such legal protection should be provided in respect of technological measures that effectively restrict acts not authorised by the rightholders of any copyright, rights related to copyright or the sui generis right in databases without, however, preventing the normal operation of electronic equipment and its technological development. Such legal protection implies no obligation to design devices, products, components or services to correspond to technologi-

cal measures, so long as such device, product, component or service does not otherwise fall under the prohibition of Article 6. Such legal protection should respect proportionality and should not prohibit those devices or activities which have a commercially significant purpose or use other than to circumvent the technical protection. In particular, this protection should not hinder research into cryptography.

(49) The legal protection of technological measures is without prejudice to the application of any national provisions which may prohibit the private possession of devices, products or components for the circumvention of technological measures.

(50) Such a harmonised legal protection does not affect the specific provisions on protection provided for by Directive 91/250/EEC. In particular, it should not apply to the protection of technological measures used in connection with computer programs, which is exclusively addressed in that Directive. It should neither inhibit nor prevent the development or use of any means of circumventing a technological measure that is necessary to enable acts to be undertaken in accordance with the terms of Article 5(3) or Article 6 of Directive 91/250/EEC. Articles 5 and 6 of that Directive exclusively determine exceptions to the exclusive rights applicable to computer programs.

(51) The legal protection of technological measures applies without prejudice to public policy, as reflected in Article 5, or public security. Member States should promote voluntary measures taken by rightholders, including the conclusion and implementation of agreements between rightholders and other parties concerned, to accommodate achieving the objectives of certain exceptions or limitations provided for in national law in accordance with this Directive. In the absence of such voluntary measures or agreements within a reasonable period of time, Member States should take appropriate measures to ensure that rightholders provide beneficiaries of such exceptions or limitations with appropriate means of benefiting from them, by modifying an implemented technological measure or by other means. However, in order to prevent abuse of such measures taken by rightholders, including within the framework of agreements, or taken by a Member State, any technological measures applied in implementation of such measures should enjoy legal protection.

(52) When implementing an exception or limitation for private copying in accordance with Article 5(2)(b), Member States should likewise promote the use of voluntary measures to accommodate achieving the objectives of such exception or limitation. If, within a reasonable period of time, no such voluntary measures to make reproduction for private use possible have been taken, Member States may take measures to enable beneficiaries of the exception or limitation concerned to benefit from it. Voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, as well as measures taken by Member States, do not prevent rightholders from using technological measures which are consistent with the exceptions or limitations on private copying in national law in accordance with Article 5(2)(b), taking account of the condition of fair compensation under that provision and the possible differentiation between various conditions of use in accordance with Article 5(5), such as controlling the number of reproductions. In order to prevent abuse of such measures, any technological measures applied in their implementation should enjoy legal protection.

(53) The protection of technological measures should ensure a secure environment for the provision of interactive on-demand services, in such a way that members of the public may access works or other subject-matter from a place and at a time individually chosen by them. Where such services are governed by contractual arrangements, the first and second subparagraphs of Article 6(4) should not apply. Non-interactive forms of online use should remain subject to those provisions.

(54) Important progress has been made in the international standardisation of technical systems of identification of works and protected subject-matter in digital format. In an increasingly networked environment, differences between technological measures could lead to an incompatibility of systems within the Community. Compatibility and interoperability of the different systems should be encouraged. It would be highly desirable to encourage the development of global systems.

(55) Technological development will facilitate the distribution of works, notably on networks, and this will entail the need for rightholders to identify better the work or other subject-matter, the author or any other rightholder, and to provide information about the terms and conditions of use of the work or other subject-matter in order to render easier the management of rights

attached to them. Rightholders should be encouraged to use markings indicating, in addition to the information referred to above, inter alia their authorisation when putting works or other subject-matter on networks.

(56) There is, however, the danger that illegal activities might be carried out in order to remove or alter the electronic copyright-management information attached to it, or otherwise to distribute, import for distribution, broadcast, communicate to the public or make available to the public works or other protected subject-matter from which such information has been removed without authority. In order to avoid fragmented legal approaches that could potentially hinder the functioning of the internal market, there is a need to provide for harmonised legal protection against any of these activities.

(57) Any such rights-management information systems referred to above may, depending on their design, at the same time process personal data about the consumption patterns of protected subject-matter by individuals and allow for tracing of on-line behaviour. These technical means, in their technical functions, should incorporate privacy safeguards in accordance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data(10).

(58) Member States should provide for effective sanctions and remedies for infringements of rights and obligations as set out in this Directive. They should take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for should be effective, proportionate and dissuasive and should include the possibility of seeking damages and/or injunctive relief and, where appropriate, of applying for seizure of infringing material.

(59) In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network. This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States.

(60) The protection provided under this Directive should be without prejudice to national or Community legal provisions in other areas, such as industrial property, data protection, conditional access, access to public documents, and the rule of media exploitation chronology, which may affect the protection of copyright or related rights.

(61) In order to comply with the WIPO Performances and Phonograms Treaty, Directives 92/100/EEC and 93/98/EEC should be amended,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I
OBJECTIVE AND SCOPE

Article 1
Scope

1. This Directive concerns the legal protection of copyright and related rights in the framework of the internal market, with particular emphasis on the information society.

2. Except in the cases referred to in Article 11, this Directive shall leave intact and shall in no way affect existing Community provisions relating to:

   (a) the legal protection of computer programs;

   (b) rental right, lending right and certain rights related to copyright in the field of intellectual property;

   (c) copyright and related rights applicable to broadcasting of programmes by satellite and cable retransmission;

   (d) the term of protection of copyright and certain related rights;

   (e) the legal protection of databases.

CHAPTER II
RIGHTS AND EXCEPTIONS

Article 2
Reproduction right

Member States shall provide for the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part:

(a) for authors, of their works;

(b) for performers, of fixations of their performances;

(c) for phonogram producers, of their phonograms;

(d) for the producers of the first fixations of films, in respect of the original and copies of their films;

(e) for broadcasting organisations, of fixations of their broadcasts, whether those broadcasts are transmitted by wire or over the air, including by cable or satellite.

Article 3
Right of communication to the public of works and right of making available to the public other subject-matter

1. Member States shall provide authors with the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them.

2. Member States shall provide for the exclusive right to authorise or prohibit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them:

   (a) for performers, of fixations of their performances;

   (b) for phonogram producers, of their phonograms;

   (c) for the producers of the first fixations of films, of the original and copies of their films;

   (d) for broadcasting organisations, of fixations of their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite.

3. The rights referred to in paragraphs 1 and 2 shall not be exhausted by any act of communication to the public or making available to the public as set out in this Article.

Article 4
Distribution right

1. Member States shall provide for authors, in respect of the original of their works or of copies thereof, the exclusive right to authorise or prohibit any form of distribution to the public by sale or otherwise.

2. The distribution right shall not be exhausted within the Community in respect of the original or copies of the work, except where the first sale or other transfer of ownership in the Community of that object is made by the rightholder or with his consent.

Article 5
Exceptions and limitations

1. Temporary acts of reproduction referred to in Article 2, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:

   (a) a transmission in a network between third parties by an intermediary, or

   (b) a lawful use

   of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2.

2. Member States may provide for exceptions or limitations to the reproduction right provided for in Article 2 in the following cases:

   (a) in respect of reproductions on paper or any similar medium, effected by the use of any kind of photographic technique or by some other process having similar effects, with the exception of sheet music, provided that the rightholders receive fair compensation;

   (b) in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the rightholders receive fair compensation which takes account of the application or non-application of technological measures

referred to in Article 6 to the work or subject-matter concerned;

(c) in respect of specific acts of reproduction made by publicly accessible libraries, educational establishments or museums, or by archives, which are not for direct or indirect economic or commercial advantage;

(d) in respect of ephemeral recordings of works made by broadcasting organisations by means of their own facilities and for their own broadcasts; the preservation of these recordings in official archives may, on the grounds of their exceptional documentary character, be permitted;

(e) in respect of reproductions of broadcasts made by social institutions pursuing non-commercial purposes, such as hospitals or prisons, on condition that the rightholders receive fair compensation.

3. Member States may provide for exceptions or limitations to the rights provided for in Articles 2 and 3 in the following cases:

(a) use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author's name, is indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved;

(b) uses, for the benefit of people with a disability, which are directly related to the disability and of a non-commercial nature, to the extent required by the specific disability;

(c) reproduction by the press, communication to the public or making available of published articles on current economic, political or religious topics or of broadcast works or other subject-matter of the same character, in cases where such use is not expressly reserved, and as long as the source, including the author's name, is indicated, or use of works or other subject-matter in connection with the reporting of current events, to the extent justified by the informatory purpose and as long as the source, including the author's name, is indicated, unless this turns out to be impossible;

(d) quotations for purposes such as criticism or review, provided that they relate to a work or other subject-matter which has already been lawfully made available to the public, that, unless this turns out to be impossible, the source, including the author's name, is indicated, and that their use is in accordance with fair practice, and to the extent required by the specific purpose;

(e) use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings;

(f) use of political speeches as well as extracts of public lectures or similar works or subject-matter to the extent justified by the informatory purpose and provided that the source, including the author's name, is indicated, except where this turns out to be impossible;

(g) use during religious celebrations or official celebrations organised by a public authority;

(h) use of works, such as works of architecture or sculpture, made to be located permanently in public places;

(i) incidental inclusion of a work or other subject-matter in other material;

(j) use for the purpose of advertising the public exhibition or sale of artistic works, to the extent necessary to promote the event, excluding any other commercial use;

(k) use for the purpose of caricature, parody or pastiche;

(l) use in connection with the demonstration or repair of equipment;

(m) use of an artistic work in the form of a building or a drawing or plan of a building for the purposes of reconstructing the building;

(n) use by communication or making available, for the purpose of research or private study, to individual members of the public by dedicated terminals on the premises of establishments referred to in paragraph 2(c) of works and other subject-matter not subject to purchase or licensing terms which are contained in their collections;

(o) use in certain other cases of minor importance where exceptions or limitations already exist under national law, provided that they only concern analogue uses and do not affect the free circulation of goods and services within the Community, without prejudice to the other exceptions and limitations contained in this Article.

4. Where the Member States may provide for an exception or limitation to the right of reproduc-

tion pursuant to paragraphs 2 and 3, they may provide similarly for an exception or limitation to the right of distribution as referred to in Article 4 to the extent justified by the purpose of the authorised act of reproduction.

5. The exceptions and limitations provided for in paragraphs 1, 2, 3 and 4 shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder.

CHAPTER III
PROTECTION OF TECHNOLOGICAL MEASURES AND RIGHTS-MANAGEMENT INFORMATION

Article 6
Obligations as to technological measures

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

   (a) are promoted, advertised or marketed for the purpose of circumvention of, or

   (b) have only a limited commercially significant purpose or use other than to circumvent, or

   (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of,

   any effective technological measures.

3. For the purposes of this Directive, the expression "technological measures" means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC. Technological measures shall be deemed "effective" where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.

4. Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.

   A Member State may also take such measures in respect of a beneficiary of an exception or limitation provided for in accordance with Article 5(2)(b), unless reproduction for private use has already been made possible by rightholders to the extent necessary to benefit from the exception or limitation concerned and in accordance with the provisions of Article 5(2)(b) and (5), without preventing rightholders from adopting adequate measures regarding the number of reproductions in accordance with these provisions.

   The technological measures applied voluntarily by rightholders, including those applied in implementation of voluntary agreements, and technological measures applied in implementation of the measures taken by Member States, shall enjoy the legal protection provided for in paragraph 1.

   The provisions of the first and second subparagraphs shall not apply to works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them.

   When this Article is applied in the context of Directives 92/100/EEC and 96/9/EC, this paragraph shall apply mutatis mutandis.

Article 7
Obligations concerning rights-management information

1. Member States shall provide for adequate legal protection against any person knowingly performing without authority any of the following acts:

   (a) the removal or alteration of any electronic rights-management information;

   (b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive or under Chapter III of Directive 96/9/EC from which electronic rights-management information has been removed or altered without authority,

   if such person knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of any copyright or any rights related to copyright as provided by law, or of the sui generis right provided for in Chapter III of Directive 96/9/EC.

2. For the purposes of this Directive, the expression "rights-management information" means any information provided by rightholders which identifies the work or other subject-matter referred to in this Directive or covered by the sui generis right provided for in Chapter III of Directive 96/9/EC, the author or any other rightholder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information.

   The first subparagraph shall apply when any of these items of information is associated with a copy of, or appears in connection with the communication to the public of, a work or other subjectmatter referred to in this Directive or covered by the sui generis right provided for in Chapter III of Directive 96/9/EC.

CHAPTER IV
COMMON PROVISIONS

Article 8
Sanctions and remedies

1. Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive.

2. Each Member State shall take the measures necessary to ensure that rightholders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2).

3. Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.

Article 9
Continued application of other legal provisions

This Directive shall be without prejudice to provisions concerning in particular patent rights, trade marks, design rights, utility models, topographies of semi-conductor products, type faces, conditional access, access to cable of broadcasting services, protection of national treasures, legal deposit requirements, laws on restrictive practices and unfair competition, trade secrets, security, confidentiality, data protection and privacy, access to public documents, the law of contract.

Article 10
Application over time

1. The provisions of this Directive shall apply in respect of all works and other subject-matter referred to in this Directive which are, on 22 December 2002, protected by the Member States' legislation in the field of copyright and related rights, or which meet the criteria for protection under the provisions of this Directive or the provisions referred to in Article 1(2).

2. This Directive shall apply without prejudice to any acts concluded and rights acquired before 22 December 2002.

Article 11
Technical adaptations

1. Directive 92/100/EEC is hereby amended as follows:

   (a) Article 7 shall be deleted;

(b) Article 10(3) shall be replaced by the following: "3. The limitations shall only be applied in certain special cases which do not conflict with a normal exploitation of the subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder."

2. Article 3(2) of Directive 93/98/EEC shall be replaced by the following: "2. The rights of producers of phonograms shall expire 50 years after the fixation is made. However, if the phonogram has been lawfully published within this period, the said rights shall expire 50 years from the date of the first lawful publication. If no lawful publication has taken place within the period mentioned in the first sentence, and if the phonogram has been lawfully communicated to the public within this period, the said rights shall expire 50 years from the date of the first lawful communication to the public.

However, where through the expiry of the term of protection granted pursuant to this paragraph in its version before amendment by Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society(11) the rights of producers of phonograms are no longer protected on 22 December 2002, this paragraph shall not have the effect of protecting those rights anew."

Article 12
Final provisions

1. Not later than 22 December 2004 and every three years thereafter, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, in which, inter alia, on the basis of specific information supplied by the Member States, it shall examine in particular the application of Articles 5, 6 and 8 in the light of the development of the digital market. In the case of Article 6, it shall examine in particular whether that Article confers a sufficient level of protection and whether acts which are permitted by law are being adversely affected by the use of effective technological measures. Where necessary, in particular to ensure the functioning of the internal market pursuant to Article 14 of the Treaty, it shall submit proposals for amendments to this Directive.

2. Protection of rights related to copyright under this Directive shall leave intact and shall in no way affect the protection of copyright.

3. A contact committee is hereby established. It shall be composed of representatives of the competent authorities of the Member States. It shall be chaired by a representative of the Commission and shall meet either on the initiative of the chairman or at the request of the delegation of a Member State.

4. The tasks of the committee shall be as follows:

(a) to examine the impact of this Directive on the functioning of the internal market, and to highlight any difficulties;

(b) to organise consultations on all questions deriving from the application of this Directive;

(c) to facilitate the exchange of information on relevant developments in legislation and case-law, as well as relevant economic, social, cultural and technological developments;

(d) to act as a forum for the assessment of the digital market in works and other items, including private copying and the use of technological measures.

Article 13
Implementation

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 22 December 2002. They shall forthwith inform the Commission thereof.

When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field governed by this Directive.

Article 14
Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 15
Addressees

This Directive is addressed to the Member States.

Done at Brussels, 22 May 2001.
For the European Parliament
The President N. Fontaine
For the Council
The President M. Winberg

[3] OJ C 108, 7.4.1998, p. 6 and OJ C 180, 25.6.1999, p. 6.

[4] OJ C 407, 28.12.1998, p. 30.

[5] Opinion of the European Parliament of 10 February 1999 (OJ C 150, 28.5.1999, p. 171), Council Common Position of 28 September 2000 (OJ C 344, 1.12.2000, p. 1) and Decision of the European Parliament of 14 February 2001 (not yet published in the Official Journal). Council Decision of 9 April 2001.

[6] OJ L 178, 17.7.2000, p. 1.

[7] Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs (OJ L 122, 17.5.1991, p. 42). Directive as amended by Directive 93/98/EEC.

[8] Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (OJ L 346, 27.11.1992, p. 61). Directive as amended by Directive 93/98/EEC.

[9] Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission (OJ L 248, 6.10.1993, p. 15).

[10] Council Directive 93/98/EEC of 29 October 1993 harmonising the term of protection of copyright and certain related rights (OJ L 290, 24.11.1993, p. 9).

[11] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (OJ L 77, 27.3.1996, p. 20).

[12] OJ L 281, 23.11.1995, p. 31.

[13] OJ L 167, 22.6.2001, p. 10.

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach

Executive Summary

I.

Security is becoming a key priority because communication and information have become a key factor in economic and societal development. Networks and information systems are now supporting services and carrying data to an extent inconceivable only a few years ago. Their availability is critical for other infrastructures such as water and electricity supply. As everybody, business, private individuals, public administrations want to exploit the possibilities of communication networks, security of these systems is becoming a prerequisite for further progress.

Against this background the Stockholm European Council on 23-24 March 2001 concluded "the Council together with the Commission will develop a comprehensive strategy on security of electronic networks including practical implementing action. This should be presented in time for the Göteborg European Council." This Communication is the European Commission's response to this request.

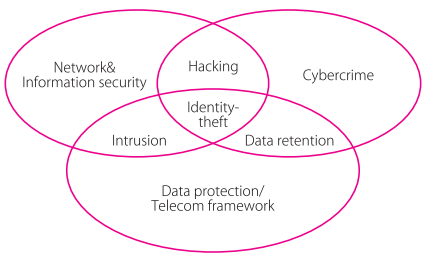
II.

Security has become a key challenge for policy makers, but finding an adequate policy response is becoming an increasingly complex task. Communication services are no longer offered by state-owned telecommunications operators but on a competitive basis by many private operators and service providers; and increasingly on a European and global level. Networks are converging: they are able to support the same services, they are increasingly interconnected, and they partly use the same infrastructure.

In order to ensure a minimum level of security, a substantial body of legislation as part of the telecommunications framework and data protection law have been put in place both at national and EU level. These legal provisions need to be applied effectively in a rapidly changing environment. They will also need to evolve in the future as can be seen by the proposed new telecommunications framework or the forthcoming proposals linked to the cyber-crime discussion. Policy makers therefore need an understanding of the underlying security issues and their role in improving security.

Security has become a commodity bought and sold on the market and part of contractual agreements between parties. The implicit assumption usually made is that the price mechanism will balance the costs of providing security with the specific need for security. However many security risks remain unsolved or solutions are slow coming to the market as a result of certain market imperfections. Specific policy measures addressing these imperfections can reinforce the market process and at the same time improve the functioning of the legal framework. Such measures must be part of a European approach in order to ensure the Internal Market, to benefit from common solutions, and to be able to act effectively at global level.

The proposed policy measures with regard to network and information security have to be seen in the context of the existing telecommunications, data protection, and cyber-crime policies. A network and information security policy will provide the missing link in this policy framework. The diagram below shows these three policy areas and illustrates with a few examples how they are interrelated:



III.

Network and information security can be understood as the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions. Such events or actions could compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data as well as related services offered via these networks and systems. These security incidents can be grouped as follows:

- Electronic communication can be intercepted and data copied or modified. This can cause damage both through invasion of the privacy of individuals and through the exploitation of data intercepted.
- Unauthorised access into computer and computer networks is usually done with malicious intend to copy, modify or destroy data..
- Disruptive attacks on the Internet have become quite common and in future the telephone network may also become more vulnerable.
- Malicious software, such as viruses, can disable computers, delete or modify data. Some recent virus attacks have been extremely destructive and costly.
- Misrepresentation of people or entities can cause substantial damages, e.g. customers may download malicious software from a website masquerading as a trusted source, contracts may be repudiated, confidential information may be sent to the wrong persons.
- Many security incidents are due to unforeseen and unintentional events such as natural disasters (floods, storms, earthquakes), hardware or software failures, human error.

IV.

The proposed measures:

- *Awareness raising:* A public information and education campaign should be launched and best practices should be promoted.
- *A European warning and information system:* Member States should strengthen their Computer Emergency Response Teams (CERTs) and improve the co-ordination among them. The Commission will examine together with Member States how to best organise at European level data collection, analysis and planning of forward-looking responses to existing and emerging security threats.
- *Technology support:* Support for research and development in security should be a key element in the 6th Framework Programme

and be linked to the broader strategy for improved network and information security.

- *Support for market oriented standardisation and certification:* European standardisation organisations are invited to accelerate work on interoperability; Commission will continue support for electronic signature and the further development of IPv6 and IPSec, Commission will assess the need for a legal initiative on the mutual recognition of certificates, Member States should review all relevant security standards.
- *Legal framework:* The Commission will set up an inventory of national measures which have been taken in accordance with relevant Community law. Member States to support free circulation of encryption products. Commission will propose legislation on cybercrime.
- *Security in government use:* Member States should incorporate effective an interoperable security solutions in their e-government and e-procurement activities. Member States should introduce electronic signatures when offering public services. The Commission will strengthen its security requirements in their information and communication system;
- *International co-operation:* The Commission will reinforce the dialogue with international organisations and partners on network and information security.

The next stage is for the framework and the proposed actions to be discussed by Member States and the European Parliament. The Göteborg European Council on 15/16 June may give orientations for the way ahead.

The Commission proposes to launch a thorough discussion with industry and users on the practical details of implementing the actions proposed. Comments can be sent to eeurope@europa.eu.int by the end of August 2001. Therefore this Communication is an invitation for comments from interested parties with a view to establishing a final concrete set of actions. This could take the form of a roadmap to be developed by the end of 2001.

Network and Information Security: Proposal for a European Policy Approach

Table of contents

1. INTRODUCTION

Concerns about security of electronic networks and information systems have been growing along with the rapid increase in the number of network users and the value of their transactions. Security has now reached a critical point where it represents a prerequisite for the growth of electronic businesses and the functioning of the whole economy. Several factors have combined to push information and communication security to the top of the policy agenda in the EU:

- Governments have realised the extent to which their economies and their citizens are dependent on the effective working of communication networks and several have begun to review their security arrangements.

- The Internet has created a global connectivity linking together millions of networks, large and small, and hundreds of millions of individual PCs, and increasingly other devices including mobile phones. This has significantly reduced the costs of accessing valuable economic information for remote attackers.
- There have been some widely reported viruses released onto the Internet causing extensive damage by destroying information and denying access to the network. Such security problems are not confined to individual countries but spread quickly across Member States.
- The Lisbon and Feira European Councils recognised the Internet as a key driver in the productivity of EU economies when launching the eEurope 2002 Action Plan.

Against this background the Stockholm European Council on 23-24 March 2001 concluded "the Council together with the Commission will develop a comprehensive strategy on security of electronic networks including practical implementing action. This should be presented in time for the Göteborg European Council." This Communication is the European Commission's response to this request.

A changing environment

Whilst security has become a key challenge for policy makers, finding an adequate policy response is becoming an increasingly complex task. Only a few years ago, network security was predominantly an issue for state monopolies offering specialised services based on public networks, in particular the telephone network. Security of computer systems was limited to large organisations and focused on access controls. Establishing a security policy was a relatively straightforward task. This situation has now changed considerably because of a variety of developments in the wider market context, amongst them liberalisation, convergence and globalisation:

Networks are now mainly privately owned and managed. Communication services are offered on a competitive basis with security as part of the market offer. However many customers remain ignorant of the extent of the security risks they run when connecting to a network and are therefore making their decisions in a situation of incomplete information.

Networks and information systems are converging. They are becoming increasingly interconnected, offering the same kind of seamless and personalised services and to some extent sharing the same infrastructure. End terminals (PCs, mobile phones, etc.) have become an active element in the network architecture and can be connected to different networks.

Networks are international. A significant part of today's communication is cross border or transits through third countries (sometimes without the end-user being aware of it), so any solution to a security risk needs to take account of this. Most networks are built using commercial products from international vendors. Security products must be compatible with international standards.

Policy relevance

These developments constrain the ability of governments to influence the level of security of the electronic communications of their citizens and businesses. This does not mean however that the public sector no longer has a role for a number of reasons:

Firstly, there are several legal measures in place at Community level with specific implications for network and information security. In particular the European telecommunications and data protection framework contains provisions for operators and service providers to ensure a level of security appropriate to the involved risks.

Secondly, there are growing concerns about national security as information systems and communication networks have become a critical factor for other infrastructures (e.g. water and electricity supply) and other markets (e.g. the global finance market).

Finally, there are reasons why action by governments is required in response to imperfections in the market. Market prices do not always accurately reflect the costs and benefits of investment in improved network security and neither providers nor users always bear all the consequences of their behaviour. Control over the network is dispersed and weaknesses in one system can be exploited to attack another. The complexity of networks makes it difficult for users to assess potential dangers.

It is therefore the objective of this Communication to establish where additional or enhanced public action at European or national level is required.

Chapter 2 defines network and information security, describes the main security threats and assesses the current solutions. It aims at providing a level of understanding of network and information security

necessary to illuminate the proposed policy solutions. It is not the intention to give an exhaustive technical overview of security issues.

Chapter 3 proposes a European policy approach aimed at improving network and information security. It is based on an analysis of the need to supplement market solutions with policy actions. It lists a series of concrete policy measures, as was requested by the Stockholm European Council. The proposed policy should be seen as an integral element of the existing framework for electronic communication services and data protection and - more recently - cyber-crime policy.

2. ANALYSIS OF NETWORK AND INFORMATION SECURITY ISSUES

2.1. What is network and information security-

Networks are systems on which data are stored, processed and through which they circulate. They are composed of transmission components (cables, wireless links, satellites, routers, gateways, switches etc) and support services (domain name system including the root servers, caller identification service, authentication services, etc). Attached to networks is an increasingly wide range of applications (e-mail delivery systems, browsers, etc.) and terminal equipment (telephone set, host computers, PCs, mobile phones, personal organisers, domestic appliances, industrial machines, etc.).

The generic security requirements of networks and information systems can be considered to consist of the following interrelated characteristics:

(i) Availability - means that data is accessible and services are operational, despite possible disruptive events such as power supply cuts, natural disasters, accidents or attacks. This is particularly vital in contexts where communication network failures can cause breakdowns in other critical networks such as air transport or power supply.

(ii) Authentication - is the confirmation of an asserted identity of entities or users . Proper authentication methods are needed for many applications and services such as concluding a contract online, controlling access to certain data and services (e.g. for teleworkers) and authentication of websites (e.g. for Internet banks). Authentication must also include the possibility for anonymity, as many services do not need the identity of the user, but only reliable confirmation of certain criteria (so-called anonymous credentials) such as the ability to pay.

(iii) Integrity - is the confirmation that data which has been sent, received, or stored are complete and unchanged. This is particularly important in relation to authentication for the conclusion of contracts or where data accuracy is critical (medical data, industrial design, etc.).

(iv) Confidentiality - is the protection of communications or stored data against interception and reading by unauthorised persons. It is particularly needed for the transmission of sensitive data and is one of the requirements to address privacy concerns of users of communication networks.

All events which threaten security need to be covered, not just those with malicious intent. From a user's point of view, threats such as environmental incidents or human errors which disrupt the network are potentially as costly as malicious attacks. Network and information security can thus be understood as the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.

2.2. Overview of security threats

Companies relying on the network for sales or to organise delivery of supplies can be paralysed by a denial of service attack. Personal and financial information can be intercepted and abused. National security can be threatened. These examples give an indication of the threats of inadequate security. A distinction is made between intentional attacks (sections 2.2.1 to 2.2.5) and unintentional events (section 2.2.6). The objective of these sections is to specify the type of security risks in order to lay the basis for the establishment of a policy framework to improve security in section 3.

2.2.1. Interception of communications

Electronic communication can be intercepted and data copied or modified. Interception can be undertaken in a number of ways. These include the physical accessing of network lines, e.g. wire tapping, and

monitoring radio transmissions. The most critical points for the interception of communication traffic are the network management and concentration points, such as routers, gateways, switches and network operation servers.

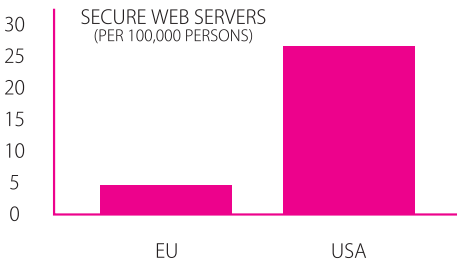
Malicious or unlawful interception of communications must be distinguished from lawful interception activities. Interception of communications for reasons of public security is authorised in specific cases for limited purposes in all EU Member States. A legal framework is in place to allow law enforcement agencies to obtain judicial orders, or in the case of two Member States, a warrant personally authorised by a senior Minister, to intercept communications.

Potential damage - Unlawful interception can cause damage both through invasion of the privacy of individuals and through the exploitation of data intercepted, such as passwords or credit card details, for commercial gain or sabotage. This is perceived to be one of the biggest inhibitors to the take-up of e-commerce in Europe.

Potential solutions - Defence against interception can be made by operators securing the network as they are required to do inter alia under Directive 97/66 EC[72] and by users encrypting data transmitted over the network.

For operators, protection of the network against potential interception is a complex and expensive task. Traditionally, telecom operators have secured the network through physical access controls to installations and guidelines for employed staff. Traffic was only occasionally encrypted. Where wireless solutions are deployed, there is an onus on ensuring that the radio transmissions are adequately encrypted. Mobile communication operators encrypt traffic between the mobile phone and the base station. The strength of encryption in most EU countries is lower than is technically feasible because of the requirements to facilitate legal interception. For the same reason the encryption can be switched on and off from the base stations without the user being aware of it.

Users can make their own decision to encrypt data or voice signals independently of network security provisions. Properly encrypted data is incomprehensible to all but the authorised recipient, even if intercepted. Encryption software and hardware is widely available for practically all types of communications[73]. Special products can encrypt a telephone conversation or a fax transmission. E-mails can be encrypted using special software or software integrated into a word processor or e-mail client. The problem for the users is that if they encrypt e-mail or voice communications the recipient must be able to understand it. Equipment or software must be interoperable. They also need to know the decryption key, which means that there should be a mechanism to receive the key including proper authentication of the key. The cost of encryption in both money and effort is significant and users often lack information about security risks and benefits and this makes it difficult for them to take the best decisions.



Source: OECD (from netcraft surveyJuly 2000)

A commonly used secure system on the Internet is the "Secure Socket Layer" (SSL). SSL encrypts the communication between a web server and a user's web browser. An inhibiting factor in the take-up of this technology, especially the strongest version (128 bit), has been the past restrictive export controls of the US The US export control regime has been recently revised following the adoption of a more liberal Community regime for the control of exports of dual use items and technologies[74]. Statistics indicate that the number of secure web servers in Europe lags far behind the US (see graph).

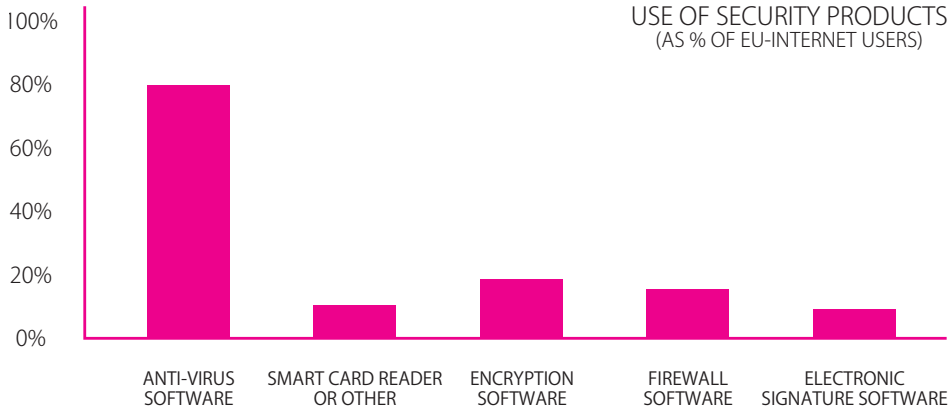
Operators, users and producers face the problem of competing and non-interoperable standards. For example in the secure e-mail field, two standards[75] are competing to become dominant. Europe's influence here has been limited. The result is a profusion of non-European products that implement these standards and where access for European users

72 Directive on data protection in telecommunications (OJ L 24 of 30.1.1998).

73 See Commission Communication on "Ensuring security and trust in electronic communication", 8 October 1997, COM (1997) 503 final.

74 Council Regulation (EC) N° 1334/2000 setting up a Community regime for the control of exports of dual use items and technologies (OJ L 159 of 30.06.2000).

75 S-MIME (secure multiple Internet mail extensions) and OpenPGP (Pretty Good Privacy) are both IETF (Internet Engineering Task Force) standards.



Source: Eurobarometer (Feb 2001)

depends on the export control policy of the United States. While there is concern in relation to the level of security offered by many of these products (c.f. Echelon[76]), some EU governments are considering the use of open source software to increase the level of confidence in encryption products. However, this is in the pilot stage[77], not yet co-ordinated and market forces may simply be stronger than isolated government efforts. This issue can be addressed by conducting a comprehensive evaluation of both the commercial and open-source products.

2.2.2. Unauthorised access into computers and computer networks

Unauthorised access to a computer or network of computers is usually done with malicious intent to copy, modify or destroy data. Technically this is called intrusion and can be done in many ways including exploiting inside information, dictionary attacks, brute force attacks (exploiting people's tendency to use predictable passwords), social engineering (exploiting people's tendency to disclose information to seemingly trustworthy people) and password interception. It is often performed from within the organisations (inside attacks).

Potential damage - Some unauthorised intrusion is motivated by intellectual challenge rather than monetary gain. However, what began as a nuisance activity (often described as 'hacking') has highlighted the vulnerabilities of information networks and motivated those with criminal or malicious intent to exploit these weaknesses. Protection against unauthorised access to their personal information, including their financial details, bank accounts and health information, is a right of individuals. For the public sector and industry, the threats range from economic espionage to the potential modification of internal or public data, including the corruption of web sites.

Potential solutions - The most common methods of protecting against unauthorised access are password controls and installation of firewalls. However, these give only limited protection and need to be complemented by other security controls which could include attack recognition, intrusion detection and application level controls (including those involving smart cards). The effectiveness of the controls is dependent on how their functionality matches the risks related to a specific environment. A balance must be achieved between network protection and the advantages of free access. Due to rapid changes and consequent new threats to networks there is a need for ongoing independent review of network security controls. Until users and providers are fully aware of the potential vulnerability of their network, potential solutions will remain unexplored. An overview of the current use of security products in the European Union is provided in the graph "Use Of Security Products" (statistics are based on a survey carried out in February 2001 in the context of the eEurope 2002 benchmarking exercise).

76 The ECHELON system is allegedly used to intercept ordinary e-mail, fax, telex and telephone communications carried over the world's telecommunications networks. See also the activities of the European Parliament Temporary Committee on Echelon at http://www.europarl.eu.int/committees/echelon_home.htm

77 The German government is funding a project based on the OpenPGP standard and is called GNUPG (http://www.gnupg.org).

2.2.3. Network disruption

Networks are now largely digitised and controlled by computers. In the past a common reason for network disruption was a failure in the computer system that controls the network and attacks on networks were mainly directed towards these computers. Nowadays, the most disrupting attacks tend to exploit the weaknesses and vulnerabilities of network components (operating systems, routers, switches, name servers, etc.).

Whilst disruptive attacks on the telephone system have not been a major concern in the past, attacks on the Internet are quite common. This is due to the fact that telephone control signals are separated from traffic and can be protected whereas the Internet allows users to reach the key management computers. However, the telephone network may become more vulnerable in future as it will integrate key elements of the Internet and its control plan will be opened to others.

Attacks may take various forms:

- Name server attacks: The Internet depends on the operation of the Domain Name System (DNS) through which user-friendly names (e.g. europa.eu.int) are translated into abstract network addresses (e.g. IP n° 147.67.36.16) and vice versa. If part of the DNS fails, some web sites cannot be located and email delivery systems may stop working. Corruption at the level of DNS root servers or other top level name servers could lead to widespread disruption. Earlier this year some vulnerabilities were discovered in the software on which most name servers operate[78].
- Routing attacks: Routing in the Internet is highly decentralised. Each router periodically informs neighbouring routers about which networks it knows and how to reach them. The weakness is that this information cannot be verified because, by design, each router's knowledge of network topology is minimal. In consequence, any router can represent itself as a best path to any destination as a way of intercepting, blocking or modifying traffic to that destination.
- Flooding and denial of service attacks: These forms of attack disrupt the network by overloading it with artificial messages which deny or reduce legitimate access. It is similar to fax machines being blocked by long and repeated messages. Flooding attacks attempt to overload web servers or the handling capacity of Internet Service Providers (ISPs) with automatically generated messages.

Potential damage - Interruptions have been damaging for certain high-profile websites. Some studies have calculated several hundreds of millions of Euro of damage from a recent attack, in addition to the intangible damage to reputation. Increasingly companies rely on the availability of their websites for their business and those companies that depend on it for 'just in time' supply are particularly vulnerable.

Potential solutions - Attacks on DNS servers are, in principle, easily dealt with by extending the DNS protocols, for example using secure DNS extensions based on public key cryptography. However, this involves installing new software on client machines and has not been widely deployed. Also, the administrative process required to enhance the trust between DNS domains needs to become more effective.

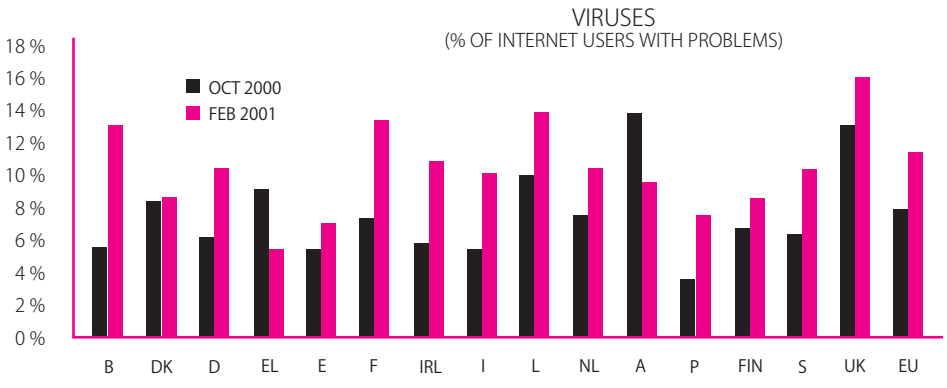
Attacks on the routing system are much harder to defend. The Internet was designed to maximise flexibility in routing as this reduces the probability of service being lost if one part of the network infrastructure breaks down. No effective means exist to secure routing protocols, especially on backbone routers.

The volume of data transmitted does not allow for detailed filtering as such verification would bring the networks to a halt. For that reason only basic filtering and access control functions are performed by the networks, whereas more specific security functions (e.g. authentication, integrity, encryption) are placed at the boundaries of the networks i.e. on the terminals and network servers that act as end points.

2.2.4. Execution of malicious software that modifies or destroys data

Computers run with software. Software can unfortunately also be used to disable a computer, to delete or modify data. As the above descriptions show, if such a computer is part of the network management its malfunctioning can have far-reaching effects. A virus is one form of malicious software. It is a program that reproduces its own code by attaching itself to other programs in such a way that the virus code is executed when the infected computer program is executed.

78 Source CERT/CC at http://www.cert.org/advisories/CA-2001-02.html



Source: Eurobarometer

There are various other types of malicious software: some damage only the computer on which they are copied and others spread themselves to other networked computers. For instance there are programmes (dramatically called 'logic bombs') that lie dormant until triggered by some event such as a specific date, - Friday the 13th - is often used. Other programmes appear to be benign but when opened release a malicious attack (therefore called 'Trojan Horses'). Other programmes (called 'worms') do not infect other programs as a virus will, but instead make copies of themselves, which consequently create even more copies to eventually swamp the system.

Potential damage - Viruses can be very destructive as illustrated by the high costs associated with some recent attacks (e.g. 'I Love you', 'Melissa' and 'Kournikova'). The chart "Viruses" gives an overview of the increase of viruses EU Internet users have encountered between October 2000 and February 2001 (by Member State). On average about 11 % of European Internet users have caught a virus on their home PC.

Potential solutions - The main defence is anti-virus software, which is available in various forms. For instance virus scanners and disinfectors identify and delete known viruses. Their main shortcoming is that they will not easily pick up new viruses even when updated regularly. Another example of anti-virus defence is an integrity checker. In order for a virus to infect a computer, it must change something on that system. The integrity check could identify these changes even when caused by unknown viruses.

Despite relatively well-developed defence products, problems with malicious software have increased. There are two main reasons. Firstly, the openness of the Internet allows attackers to learn from each other and develop methods to circumvent protection mechanisms. Secondly the Internet is growing and reaching more users, many of which a re unaware of the need to take precautionary measures. Security will depend on the extent to which defence software is used.

2.2.5. Malicious misrepresentation

When establishing a network connection or receiving data the user makes assumptions on the identity of their interlocutor based on the context of the communication. The network offers certain indicators but the greatest risk of attack comes from people who know the context i.e. insiders. When users dial a number or type an Internet address into the computer they should reach the expected destination. This is sufficient for many applications, but not for key business, medical, financial or official interactions which require a higher level of authentication, integrity and confidentiality.

Potential damage - Misrepresentation of people or entities can cause damage in various ways. Customers may download malicious software from a website masquerading as a trusted source. They may release confidential information to the wrong person. There is the possibility of misrepresentation leading to repudiation of contracts etc. Perhaps the greatest damage is the fact that lack of authentication is holding back potential business. Many studies have highlighted security worries as a principal reason for not doing business over the Internet. If people could be certain that their interlocutor is who they say they are, the level of confidence in Internet transactions would increase.

Potential solutions - Attempts to introduce authentication into the networks linked to the introduction of SSL is already useful in ensuring a certain level of confidentiality. Virtual Private Networks (VPN) use SSL and IPsec to enable communications to run over insecure Internet and open channels while maintaining a given security level. However, these solutions are limited in their usefulness as they are based on electronic certificates and there is no guarantee that these certificates are not forged. A third party, often referred to as 'Certification Authority' or in the e-signatures Directive[79] a 'Certification Service Provider', can offer such assurance. The problem for widespread uptake of this solution is similar to that faced in encryption - the need for interoperability and key management. In a VPN this is not a problem as proprietary solutions can be developed but for public networks it is a major barrier.

The e-signature Directive enhances the legal basis to assure easier electronic authentication in the EU. It provides a framework where the market is free to develop, but which also provides incentives to develop more secure signatures for legal recognition. The transposition of the Directive into national law is currently in process.

2.2.6. Environmental and unintentional events

Many security incidents are due to unforeseen and unintentional events caused by

- natural disasters (e.g. storms, floods, fires, earthquakes)
- third parties without any contractual relation with the operator or the user (e.g. interruption of service because of construction works)
- third parties with a contractual relation with the operator or the user (e.g. hardware or software failures in delivered components or programs)
- human error or poor management of the operator (including the service provider) or the user (e.g. problems in network management, incorrect installation of software).

Potential damage: Natural disasters cause disruption in the availability of networks. Unfortunately it is during such events that functioning communication lines are most needed. Hardware failures and poor software design can create vulnerabilities which cause immediate disruption or are exploited by attackers. Poor management of network capacity can lead to congestion that slows down or disrupts the communication channels.

In this context, a crucial question is the distribution of liabilities amongst parties. In most cases the users will have no responsibility but may find themselves with little or no possibilities for liability claims.

Potential solution: The risks of environmental incidents are known to telecommunication network operators and they have built redundancies and infrastructure protection into their networks. Increasing competition could have an ambivalent impact on the behaviour of operators. On the one hand price considerations may drive operators to reduce these redundancies and on the other hand the existence of more operators in the market as a result of liberalisation enable users to switch to another operator in case of unavailability (much like an air passenger is switched to another air line when a flight is cancelled). However relevant Community law requires that Member States take all necessary steps to ensure the availability of public networks in the event of catastrophic network breakdown or natural disasters (c.f. Interconnection Directive 97/33/EC[80] and Voice telephony Directive 98/10/EC[81]). Overall, in this area, too little is known about the level of security as a result of the increasing number of interconnected networks.

Competition amongst hardware and software vendors should exert pressure to improve the security of their products. However competition is not strong enough to drive security investments and security is not always the key element in the buying decision. Security flaws are often discovered too late, when the damage has already been done. The preservation of fair competition behaviour in the markets for information technology will create better security conditions.

The risk of human error and operating mistakes can be reduced by improved training and awareness raising. The establishment of an appropriate security policy at company level would help to reduce these risks.

2.3. New challenges

Network and information security is likely to be-

79 Directive 1999/93/EC of 13 December 1999 establishing a common framework for electronic signatures (OJ L 13 of 19.1.2000, p. 12).

80 OJ L 199 of 26.07.1997.
81 OJ L 101 of 01.04.1998.

come a key factor in the development of the information society as networking plays a larger role in economic and social life. There are two main issues to consider: the increasing potential damage and new technological developments.

(i) Networks and information systems carry more and more sensitive data and economic valuable information which will increase the incentive for attacks. These attacks can be low-level and inconsequential on a national scale - e.g. in the case of the defacement of a personal web site or the reformatting of a hard disk by a virus. However, the disruption can also be on a much more critical scale, up to the level of interference with highly sensitive communications, significant power cuts, or major loss of business through denial of service attacks or confidentiality breaches. The exact extent of actual and potential damage due to breaches in network security is difficult to assess. There is no systematic reporting system and many companies prefer not to admit encountered attacks for fear of negative publicity. Thus the evidence that exists is mainly anecdotal. Costs involved consist not just of direct costs (loss of revenue, loss of valuable information, manpower costs to restore the network), but there are many intangible costs associated with attacks - particularly loss of reputation - which are difficult to assess.

(ii) Network and information security is a dynamic issue. The speed of technology change poses permanent new challenges, problems of yesterday disappear and today's solutions are meaningless. The market offers new applications, services and products on an almost daily basis. However, there are some developments which will clearly pose significant challenges to a private and public security policy:

- Different digital objects will be transmitted on the networks such as multimedia objects, downloadable software or mobile agents with incorporated security policies. The notion of availability perceived today as the ability to use the networks will evolve in terms of authorised usage e.g. right to use a video game for a certain period, right to create a single copy of a software program, etc.
- In the future, operators of IP-networks may want to increase security by continually auditing the network traffic in order to only allow authorised traffic. Such measures however must be in accordance with relevant data protection rules.
- Users will switch to having 'always-on' Internet connections, which widen the window of opportunity for attackers and create vulnerabilities for unprotected terminals, and make it easier for attackers to avoid detection.
- Home networks connecting a variety of appliances will be widely introduced, opening up new avenues of attack and increasing user vulnerability (for example alarms could be turned off remotely).
- Large-scale introduction of wireless networks (e.g. wireless local loop, wireless local area networks, third generation mobile) will bring the challenge of effectively encrypting data transmitted over radio signals. It will therefore be increasingly problematic to require by law weak encryption of those signals.
- Networks and information systems will be everywhere, combining fixed and wireless and offering 'ambient intelligence', i.e. self-organisational functions that run automatically and make decisions formerly taken by the user. The challenge will be to avoid unacceptable vulnerabilities and integrate security into the architectures.

3. A EUROPEAN POLICY APPROACH

3.1. Rationale for public policy

Protecting communication networks is increasingly considered as a priority for policy makers mainly because of data protection, ensuring a functioning economy, national security, and the wish to promote e-commerce. This has led to a substantial body of legal safeguards in EU Directives on data protection and in the EU regulatory framework for telecommunications (as demonstrated in section 3.6). These measures however have to be applied in a rapidly changing environment of new technologies, competitive markets, convergence of networks, and globalisation. These challenges are compounded by the fact that the market will tend to under invest in security for reasons analysed below.

Network and information security is a commodity bought and sold on the market and part of the contractual agreements between parties. The market for

security products has grown substantially over the past few years. According to some studies the market for Internet security software was worth around $4.4 billion worldwide at the end of 1999[82] and will grow 23 % per annum to reach $ 8.3 billion in 2004. In Europe, the electronic communication security market is forecast to grow from $465 million in 2000 to $5.3 billion in 2006[83], with the security market for information technologies growing from $490 million in 1999 to $2.74 billion in 2006[84].

The implicit assumption usually made is that the price mechanism will balance the costs of providing security with the specific need for security. Certain users will request high security whilst others will be satisfied with a lower level of assurance - although the State may provide for a minimum level of security. Their preferences would be reflected in the price they are willing to pay for security features. However - as shown by the analysis of section 2 - many security risks remain unsolved or solutions are slow coming to the market as a result of certain market imperfections:

(i) Social costs and benefits: Investment in improved network security generates social costs and benefits which are not adequately reflected in market prices. On the cost side, market actors are not responsible for all the liabilities related to their security behaviour. Users and providers with low levels of security do not have to pay third party liability. This is like a careless car driver who is not held liable for the costs of the traffic jam that occurred as a result of his accident. Similarly, on the Internet several attacks have been mounted through the ill-protected machines of relatively careless users. Security benefits are also not fully reflected in market prices. When operators, suppliers, or service providers improve the security of their products a good deal of the benefits of this investment accrue not only to their customers but to all those directly or indirectly affected by electronic communication - basically the whole economy.

(ii) Asymmetry of information: Networks are becoming increasingly complex and are reaching a wider market that includes many users with little understanding of the technology or its potential dangers. This means users will not be fully aware of all the security risks and many operators, vendors, or service providers have difficulties assessing the existence and widespread of vulnerabilities. Many new services, applications and software offer attractive features but often these are the source of new vulnerabilities (e.g. the world wide web's success is partly due to the range of multimedia applications that can be easily downloaded but these 'plug-ins' are also an entry point for attacks). Whilst the benefits are visible, the risks are not and there are more incentives for suppliers to offer new features than greater security.

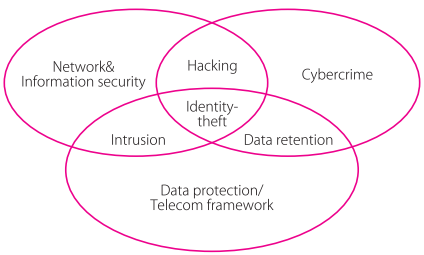
(iii) The public action problem: Operators are increasingly adopting the Internet standards or somehow linking their networks to the Internet. However, the Internet was not designed with security in mind but on the contrary was developed to ensure access to information and to facilitate its exchange. This has been the basis for its success. The Internet has become a global network of networks of unparalleled richness and diversity. Investment in security often only pays off if enough people do the same. Thus co-operation to create security solutions is required. But co-operation only works if a critical mass of players participates which is difficult to achieve as there are 'free-rider' profits to be made. Interoperability between products and services will allow for competition between security solutions. However there are substantial co-ordination costs involved as global solutions might be required and some players are tempted to impose a proprietary solution on the market. As a multitude of products and services still uses proprietary solutions there is no advantage to using secure standards which only give extra security if everyone else offers them.

As a result of these imperfections the telecommunications and data protection framework already provides for legal obligations for operators and service providers to ensure a certain level of security in communication and information systems. The rationale

82 IDC : Internet security market forecast and analysis, 2000-2004 Report W23056 - October 2000
83 Frost&Sullivan : The European Internet communication security markets, report 3717 - November 2000
84 Frost&Sullivan : The European Internet system security markets, report 3847 - July 2000

for a European policy on network and information security can be described as follows. Firstly, the legal provisions at EU level need to be applied effectively which requires a common understanding of the underlying security issues and the specific measures to be taken. The legal framework will also need to evolve in the future as already can be seen by the proposed new regulatory framework for electronic communications or the forthcoming proposals linked to the cyber-crime discussion. Secondly, certain market imperfections lead to the conclusion that market forces do not drive sufficient investment into security technology or security practice. Policy measures can reinforce the market process and at the same time improve the functioning of the legal framework. Finally, communications and information services are offered across borders. Therefore, a European policy approach is needed to ensure the Internal Market for such services, to benefit from common solutions, and to be able to act effectively on global level.

The proposed policy measures with regard to network and information security have to be seen not only in the context of the existing telecommunications and data protection legislation but also in relation to the more recent cyber-crime policies. The Commission has recently published a Communication on cyber-crime[85] which foresees, amongst other initiatives, the setting up of an EU Forum on cybercrime with the aim of enhancing mutual understanding and co-operation at EU level between all interested parties. A network and information security policy will provide the missing link in this policy framework. The diagram below shows these three policy areas and illustrates with a few examples how they are interrelated:



85 Creating a safer society by improving the security of information infrastructures and combating computer related crime, COM (2000) 890, http://europa.eu.int/ISPO/eif/internetPoliciesSite/Crime/crime1.html

3.2. Awareness raising

Too many users (private/public) are still not aware of the possible threats they encounter when using communication networks or of the solutions that already exist to tackle them. Security issues are complex and risks are often difficult, even for experts, to assess. Lack of information is one of the market imperfections that security policy should address. There is a risk that some users, alarmed by the many reports of security threats, simply choose to avoid e-commerce altogether. Others who are either uninformed or underestimate the risk may be too careless. Some companies may have an interest in underplaying potential risks, for fear of losing customers.

Paradoxically there is a huge amount of information on network and information security available on the Internet and computer magazines cover this issue quite extensively. The problem for users is to find appropriate information that is understandable, up-to-date and responds to their particular needs. The automobile industry gives a good example of how complex safety specifications can be transformed into a key marketing feature. Finally, the service providers of a publicly available telecommunications service are obliged under EU law to inform their subscribers concerning particular risks of a breach of security of the network and any possible remedies, including the costs involved (c.f. article 4 of Directive 97/66/EC).

The aim of an awareness raising initiative for citizens, administrations and businesses is therefore to provide accessible, independent and reliable information on network and information security. An open discussion on security is needed. Once awareness is assured people are free to make their own choices on the level of protection that they are comfortable with.

Proposed actions:

- Member States should launch a public information and education campaign and ongoing work needs to be upgraded. This should comprise a mass media campaign and action targeted at all stakeholders. A well-designed and effective information campaign is not cheap. Developing content that describes risk without unnecessarily alarming people and without encouraging potential hackers requires careful planning.

  The European Commission will facilitate an exchange of best practice and ensure a

certain level of co-ordination of the various national information campaigns at EU level, in particular as regards the substance of information to be provided. One element of this action would be a portal for web sites both at national and European level. Linking these portals to trusted web sites from international partners could also be envisaged.

- Member States should promote the use of best practice in security, based on existing measures such as ISO/IEC 17799 (code of practice for information security management www.iso.ch). Small and medium sized companies should be particularly targeted. The Commission will support Member States in their efforts.
- Education systems in Member States should give more emphasis on courses focused on security. The development of educational programs at all levels, for example training on the security risks of open networks and effective solutions should be encouraged to become part of computer education in schools.

  Teachers need in turn to learn about security in their own training programmes. The European Commission is supporting the development of new modules for the curricula in the context of its research programme

3.3. A European Warning and Information System

Even when users are aware of security risks they will still need to be alerted to new threats. Malicious attackers will almost inevitably find new vulnerabilities to circumvent state-of-the art protection. The industry is permanently developing new software applications and services, offering better quality of services, making the Internet more attractive, but in the process unintentionally opening up new vulnerabilities and risks.

Even experienced network engineers and security experts are often surprised by the novelty of some attacks. Therefore an early warning system is needed that can rapidly alert all users, together with a source of quick and trustworthy advice on how to tackle attacks. Business also needs a confidential mechanism to report attacks without risking to loose public confidence. This needs to be complemented by a more extensive forward-looking security analysis, bringingtogether evidence and assessing the risks with the benefit of a broader view.

Much work is done in this area by public and private "Computer Emergency Response Teams" (CERTs) or similar entities. For instance Belgium has established a virus alert system allowing Belgian citizens to be informed of virus threats within two hours. However CERTs operate differently in each Member State making co-operation complex. The existing CERTs are not always well equipped and their tasks are often not clearly defined. World-wide co-ordination is done through CERT/CC, which is part-funded by the US government and CERTs in Europe are dependent on the information release policy of CERT/CC and others.

As a result of these complexities European co-operation has so far been limited. Co-operation is essential to ensure early warning throughout the Union through the instantaneous exchange of information on the first signs of attack in one country. Therefore co-operation with the CERT system within the European Union should be strengthened as a matter of urgency. A first action aiming at strengthening the public/private co-operation on dependability of information infrastructures (including the development of early warning systems) and improving co-operation amongst CERTS has been agreed in the context of the eEurope action plan.

Proposed actions:

- Member States should review their CERT system with a view to strengthening the equipment and competence of existing CERTS. In support of national efforts the European Commission will develop a concrete proposal to strengthen co-operation within the European Union. This will include project proposals in the framework of the TEN Telecom program to ensure effective networking and the establishment of accompanying measures in the IST programme to facilitate exchange of information.
- Once the CERT network is established at EU-level it should be connected to similar institutions world wide, for example the proposed G8 incident reporting system.
- The Commission proposes to examine with Member States how to best organise at European level data collection, analysis and planning of forward-looking responses to existing and emerging security threats. The organisational nature of a possible structure is a matter of discussion with the Member States.

3.4. Technology support

Investment in network and information security solutions is currently sub-optimal. This is the case both in terms of technology uptake and research into new solutions. In a context where emerging new technologies inevitably bring with them new risks, on-going research is vital.

Network and information security is already included in the Information Society Technologies (IST) Programme of the EU's 5th Framework Research Programme (representing EUR3.6 billion over four years), with approximately EUR30 million to be spent in collaborative research on security related technologies in 2001/2002.

Research at technical level on cryptography is well advanced in Europe. The Belgian algorithm called 'Rijndael' won the Advanced Encryption Standard competition organised by the US standardisation institute (NIST). The NESSIE (New European Schemes for Signature, Integrity and Encryption) IST-project has launched an enlarged competition on encryption algorithms fulfilling the requirements of new multimedia applications, mobile commerce and smart cards.

Proposed actions:

- The Commission is proposing to include security in the future 6th Framework programme, which is currently under discussion in Council and Parliament. For this spending to be optimal, it should be linked to a broader strategy for improved network and information security. Research supported by this program should address the key security challenges posed by the "all-digital" world and by the need to secure the rights of individuals and communities. It will focus on basic security mechanisms and their interoperability, dynamic security processes, advanced cryptography, privacy enhancement technologies, technologies to handle digital assets and technologies for dependability to support business and organisational functions in dynamic and mobile systems.
- Member States should actively promote the use of 'pluggable'[86] strong encryption products. Security solutions based on 'plug in encryption' must be available as an alternative to those embedded in operating systems.

86 'Pluggable' means that an encryption software commodity can be easily installed and made fully operational on top of operating systems.

3.5. Support for market oriented standardisation and certification

For security-enhancing solutions to be effective they have to be commonly implemented by relevant market players and preferably based on open international standards. One of the main barriers to the uptake of many security solutions, for instance electronic signatures, has been the lack of interoperability between different implementations. If two users wish to communicate securely across different environments interoperability must be ensured. The use of standardised protocols and interfaces should be encouraged, including the application of conformity testing as well as "interoperability" events. Open standards, preferably based on open source software may contribute to faster fault repair as well as greater transparency.

Also, information security evaluation contributes to the users' trust and confidence. The use of common criteria has facilitated mutual recognition as a method for evaluation in many countries[87] and these countries have also entered into an arrangement with the US and Canada for mutual recognition for IT security certificates.

Certification of business processes and information security management systems is supported by the European co-operation for accreditation (EA)[88]. Accreditation of certification bodies enhances confidence in their competence and impartiality, thus promoting the acceptance of their certificates throughout the Internal Market.

In addition to certification, interoperability tests should also be carried out. An example of this approach is the European Electronic Signatures Standardisation Initiative (EESSI), which is developing consensus solutions in support of the EU directive on electronic signatures. Other examples are the smart card initiative in eEurope and the Public Key Infrastructure (PKI) implementation initiatives launched within the Interchange of Data between Administration program (IDA).

There is no lack of standardisation efforts but a great number of competing standards and specifications that lead to fragmentation of the market and

87 Council Recommendation 95/144/EC on common information technology security evaluation criteria (implemented in the majority of EU Member States).

88 European co-operation for Accreditation between accreditation bodies from 25 EU, EFTA and candidate countries.

to non-interoperable solutions. Therefore current standardisation and certification activities need better co-ordination also to keep pace with the introduction of new security solutions. Harmonisation of specifications will lead to increased interoperability at the same time enabling swift implementation by market players.

Proposed actions:

- European standardisation organisations are invited to accelerate the work on interoperable and secure products and services within an ambitious and fixed timetable. Where necessary new forms of deliverables and procedures should be followed in order to speed up the work and to strengthen the co-operation with consumer representatives and the commitment from market players.
- The Commission will continue to support, notably through the IST and IDA programs, the use of electronic signatures, the implementation of user friendly interoperable PKI solutions and the further deployment of IPv6 and IPSec[89] (as provided for in the eEurope 2002 Action Plan).
- Member States are invited to promote the use of certification and accreditation procedures on generally accepted European and international standards favouring mutual recognition of certificates. The Commission will assess the need for a legal initiative on the mutual recognition of certificates before the end of 2001.
- European market players are encouraged to participate more actively in European (CEN, Cenelec, ETSI) and international standardisation activities (Internet Engineering Task Force (IETF) , World Wide Web Consortium (W3C)).
- Member States should review all relevant security standards. Competitions could be organised together with the Commission, for European encryption and security solutions with a view to stimulate internationally agreed standards.

89 IPv6 is an Internet protocol increasing the number of possible IP addresses, optimising the traffic routing of messages and enhancing the possibilities to deploy IPSec. IPSec is another Inernet protocol aiming to provide confidentiality, to prevent packets from being viewed except by the receiving host and to provide authentication and integrity to guarantee that the data in the packet is authentic and from the correct sender.

3.6. Legal Framework

There are several legal texts influencing security in communication networks and information systems of which the regulatory framework for telecommunications is the most comprehensive. Because of the convergence of networks, security issues are now bringing together regulation and regulatory traditions from various sectors. These include telecommunications (encompassing all communication networks) which is being regulated and deregulated at the same time, the largely unregulated computer industry[90], the Internet which has functioned mainly on the basis of a 'hands off' approach and e-commerce which is increasingly subject to specific regulation. In relation to security, provisions regarding third-party liability, cyber-crime, electronic signatures, data protection and export regulations are relevant. Of these various provisions the data protection directives, the regulatory framework for telecommunications, and several legal initiatives in the context of the cyber-crime Communication are of particular relevance.

Protection of privacy is a key policy objective in the European Union. It was recognised as a basic right under Article 8 of the European Convention on human rights[91]. Articles 7 and 8 of the Charter of Fundamental Rights of the European Union[92] also provide the right to respect for family and private life, home and communications and personal data.

The Data Protection Directives[93] and more particularly article 5 of the Telecommunications Data Protection Directive[94] oblige Member States to ensure the confidentiality in public telecommunications networks, as well as publicly available telecommunication services. In addition, and in order to put article 5 into practice, under article 4 of the same Directive providers of public services and networks are required to take appropriate technical and organi-

90 There are security requirements regarding electrical components of a computer, but no requirements as to security of data handled by a computer.

91 http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/con10881.htm#HD_NM_15

92 OJ C 364 of 18.12.2000, www.ue.eu.int/df/docs/en/CarteEN.pdf

93 Directives 95/46/EC (OJ L281 of 23.11.1995) and 97/66/EC (OJ L24 of 30.1.1998) http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf

94 'Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunication network and publicly available telecommunication services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised, in accordance with article 14 (1)'.

sational measures to safeguard the security of their services. In further accordance with the article, these measures must ensure a level of security that is appropriate to the risk presented, in view of the state of the art and the cost of their implementation. This means all network operators have a legal obligation to protect communications against unlawful interception. The pan-European nature of services and greater transborder competition will call for more harmonisation of these provisions.

The general Data Protection Directive 95/46/EC requires in article 17 controllers and processors to take measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected in particular if the processing involves the transmission of data over a network. They must implement appropriate technical and organisational measures against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.. These provisions have implications for security requirements on networks and information systems used by those persons and organisations for instance e-commerce service providers. The pan-European nature of services and greater trans-border competition lead to increasing need for specification of the means to put in place in order to comply with these provisions.

The EU framework for telecommunications services contains several provisions with respect to 'security of network operations' (meaning availability of networks in case of emergency) and 'network integrity' (meaning ensuring normal operation of interconnected networks)[95]. The Commission proposed a new regulatory framework for electronic communication services in July 2000 (which is currently subject to the co-decision procedure and, therefore, discussed in the European Parliament and in the Council). The Commission proposals restate in essence - though with modifications - the existing provisions as regards network security and integrity.

The existing legal framework does, therefore, besides covering the specific topics addressed in each legal text, also concern certain aspects of networks and information systems as addressed by the present communication.

The cyber-crime Communication has triggered a debate in the European Union on how to react to criminal activities that use computers and electronic networks. Discussions will continue between all interested parties in the framework of the EU Forum to be set up shortly as announced in the Commission Communication on cyber-crime. Member States' criminal laws should cover unauthorised access to computer networks including the violation of personal data security. At present, there is no approximation of criminal law at the level of the European Union in this area. This can lead to problems investigating these offences and fails to provide a strong deterrent to those contemplating hacking or similar attacks. Approximation of criminal laws against intrusion into computer networks is also important to facilitate judicial co-operation between Member States.

The legitimate concerns about cyber-crime necessitate effective law enforcement investigations. However these legal concerns should not create solutions where legal requirements lead to weakening the security of communication and information systems.

Proposed actions:

- A common understanding of the legal implications of security in electronic communications is required. For this purpose the Commission will set up an inventory of national measures that have been taken in accordance with relevant Community law.
- Member States and the Commission should continue to support free circulation of encryption products and services through closer harmonisation of administrative export procedures and further relaxation of export controls.
- The Commission will propose a legislative measure under Title VI of the Treaty on the European Union to approximate national criminal laws relating to attacks against computer systems, including hacking and denial of service attacks. .

3.7. Security in government use

The eEurope 2002 Action Plan aims to encourage more effective and efficient interaction between citizens and the public administration. As much of the information exchanged between citizens and the administration is of a personal or confidential nature (medical, financial, legal etc.), security is vital to ensuring successful uptake. Furthermore, the development of e-government makes public adminis-

95 Commission Liberalisation Directive 90/388/EC, Interconnection Directive 97/33/EC, Voice Telephony Directive 98/10/EC.

trations both potential exemplars in demonstrating effective secure solutions and market actors with the ability to influence developments through their procurement decisions.

The issue for public administrations is not just to procure information and communication technology systems with security requirements but to develop a culture of security in the organisation. This can be accomplished through the establishment of 'organisational security policies' tailored to the needs of the institution.

Proposed actions:

- Member States should incorporate effective and interoperable information security solutions as a basic requirement in their e-government and e-procurement activities.
- Member States should introduce electronic signatures when offering online public services
- In the framework of the e-Commission, the Commission will take a series of measures to strengthen the security requirements in its information and communications systems.

3.8. International co-operation

Just as the communications using the networks easily cross borders in a fraction of a second, so do the associated security problems. The network is only as secure as the weakest link and Europe cannot isolate itself from the rest of the global network. Consequently addressing security issues require international co-operation.

The European Commission is already contributing to the work of international fora such as G8, OECD, UN. The private sector is dealing with security issues in their organisations such as the Global Business Dialogue (www.GBDe.org) or the Global Internet Project (www.GIP.org). A continuing dialogue between these organisations will be essential for global security.

Proposed action:

- The Commission will reinforce the dialogue with international organisations and partners on network security, and in particular on the increasing dependability on electronic networks.

4. NEXT STEPS

This Communication provides the strategic outline for action in this area. It is only a first step and not yet a definitive action plan for network security in Europe. However it already makes suggestions for actions in order to establish a framework for a common European approach. The next stage is for the framework and the proposed actions to be discussed by Member States and the European Parliament. The Göteborg European Council on 15/16 June may give orientations for the way ahead.

The Commission proposes to launch a thorough discussion with industry, users and data protection authorities on the practical details of implementing the actions proposed. Comments can be sent to eeurope@cec.eu.int by the end of August 2001. Therefore this Communication is an invitation for comments from interested parties with a view to establishing a final concrete set of actions. This could take the form of a roadmap to be developed by the end of 2001.

Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security

THE COUNCIL OF THE EUROPEAN UNION,

RESPONDING TO

the Conclusions of the Stockholm European Council of 23 and 24 March 2001 that the Council together with the Commision will develop a comprehensive strategy on security of electronic networks including practical implementing action,

RECALLING

1. the Resolution of the Council of 30 May 2001 - eEurope Action Plan: Information and Network Security;
2. the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for a European Policy Approach;
3. the Communication from the Commission to the Council and the European Parliament - eEurope 2002: Impact and priorities;
4. the eEurope 2002 Action Plan endorsed by the Feira European Council of 19 and 20 June 2000;
5. Council Recommendation 95/144/EC of 7 April 1995 on common information technology security evaluation criteria(1);
6. the Council Recommandation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime(2);
7. the Communication from the Commission on creating a safer society by improving the security of information infrastructures and combating computer related crime;
8. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data(3);
9. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free meovement of such data(4);
10. Directive 97/33/EC of the European Parliament and of the Council of 30 June 1992 on interconnection with telecommunications with regard to ensuring universal service and interoperability through application of the principles of open network provision (ONP)(5);
11. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(6);
12. Directive 98/10/EC of the European Parliament and of the Council of 26 February 1998 on the application of open network provision (ONP) to voice telephony and on universal service for telecommunications in a competitive environment(7);
13. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures(8);

WHEREAS:

(1) Networks and communication systems have become a key factor in economic and social development and their availability and integrity is crucial to essential infrastructures, as well as to most public and private services and the economy as a whole.

(2) In the light of the increasingly important role played in the economy by electronic services, the security of networks and information systems is of growing public interest.

(3) The security of transactions and data has become essential for the supply of electronic services, including e-commerce and online public services, and low confidence in security could slow down the widespread introduction of such services.

(4) There is a need for individuals, businesses, administrations, and other organisations to protect their own information, data and communication systems by deploying effective security technologies, where appropriate.

(5) The private sector, acting in a competitive market environment, and through its capacity to in-

novate offers a variety of solutions adapted to genuine market needs.

(6) The complex nature of network and information security means that in developing policy measures in this field, public authorities must take into account a range of political, economic, organisational and technical aspects, and be aware of the decentralised and global character of communication networks.

(7) Policy measures can be more effective if they are part of a European approach, respect the effective functioning of the Internal Market, build on increased cooperation between Member States and internationally, and support innovation and the ability of European enterprises to compete at global level.

(8) A substantial body of legislation relevant to network and information security is already in place, notably as part of the Union's legal framework for telecommunications, electronic commerce and electronic signatures.

(9) There are legal requirements imposed on providers of telecommunications services to take appropriate technical and organisational measures to safeguard the security of their services; these measures shall ensure a level of security appropriate to the risk represented.

(10) The international standard ISO-15408 (Common criteria) has become a recognised system for defining security requirements for computer and network products and evaluating whether a particular product meets those requirements.

(11) The international standard ISO-17799 (Information technology - Code of practice for information security management) and similar national guidelines are becoming recognised practice for security management in private and public organisations.

(12) Internet infrastructure should permit a high degree of access to networks and services, and be managed and operated in a robust and secure manner, e.g. by the adoption of open standards and internet security protocols;

CONSIDERING, in line with Council Resolution of 30 May 2001 on the "eEurope Action Plan: Information and Network Security", that network and information security is about

- ensuring the availability of services and data,
- preventing the disruption and unauthorised interception of communications,
- confirmation that data which has been sent, received or stored are complete and unchanged,
- securing the confidentiality of data,
- protection of information systems against unauthorised access,
- protecting against attacks involving malicious software,
- securing dependable authentication;

THEREFORE ASKS THE MEMBER STATES

1. by the end of 2002 to launch or strengthen information and education campaigns to increase awareness of network and information security; to specifically target such actions at business, private users and public administrations; to develop such awareness raising actions closely with the private sector, including inter alia internet service providers, and to encourage private sector-led initiatives;
2. to promote best practices in information security management notably in small and medium sized enterprises based, where appropriate, on internationally recognised standards;
3. by the end of 2002 to strengthen or promote the importance of security concepts as part of computer education and training;
4. by mid 2002 to review the effectiveness of national arrangements regarding computer energency response, which could include virus alert systems, with a view to strengthening, where necessary, their ability to prevent, detect, and react efficiently at national and international level against network and information systems disruption and attack;
5. to promote the use of the common criteria standard (ISO-15408) and to facilitate mutual recognition of related certificates;
6. by the end of 2002 to take significant steps towards effective and interoperable security solutions based on recognised standards where possible - which could include open source software - in their e-govemment and e-procurement activities, and towards the introduction of electronic signatures to allow those public services that require strong authentication also to be offered on-line;
7. where they choose to introduce electronic and biometrics identification systems for public or official use, to cooperate where appropriate on

technological developments and to examine any possible interoperability requirements;

8. with a view to facilitating Community and international cooperation, to exchange information with each other and with the Commission on the bodies primarily responsible within their territory for network and information security matters;

WELCOMES THE INTENTION OF THE COMMISSION

1. in 2002 to facilitate an exchange of best practice regarding awareness-raising actions and to draw up an initial inventory of the various national information campaigns;

2. in 2002 to make proposals to reinforce the Community's dialogue and cooperation with international organisations and partners on network security, in particular on the implications of the increasing dependency on electronic communication networks; and in this context to propose, by the end of 2002, a strategy for a more stable and secure operation of the Internet infrastructure;

3. by the end of 2002 to propose adequate measures to promote the ISO 15408 (Common Criteria) standard, to facilitate mutual recognition of certificates, and to improve the process by which products are evaluated, i.e. by developing adequate protection profiles;

4. by the end of 2002 to prepare a report on technologies and applications of electronic and biometric authentication of identity with a view to improving the effectiveness of such systems, in particular through interoperability;

5. by mid 2002 to make proposals - after consultation with the Member States and the private sector - for the establishment of a cyber-security task force to build on national efforts to both enhance network and information security and to enhance Member States' ability, individually and collectively, to respond to major network and information security problems;

6. by the end of 2002, to explore, in collaboration with Member States, the possible options for mechanisms by which Member States and the Commission can exchange information and experience on their achievement of the objectives of this Resolution, taking into account the cross-pillar dimension of network and information security, and to explore how the private sector can be best involved in this exchange of information and experience;

WELCOMES the increased focus of European research activities on security matters;

STRESSES the need for more research activities, in particular on security mechanisms and their interoperability, network reliability and protection, advanced cryptography, privacy enhancement technologies and security in wireless communications;

CALLS UPON

- suppliers and service providers to strengthen security as an integral and essential part of their products and services;
- the European private sector suppliers and service providers and their representative groupings to participate more actively in international standardisation activities and organise themselves into appropriate fora to contribute to the objectives of this resolution.

[1] OJ L 93, 26.4.1995, p. 27.

[2] OJ C 187, 3.7.2001, p. 5.

[3] OJ L 8, 12.1.2001, p. 1.

[4] OJ L 281, 23.11.1995, p. 31.

[5] OJ L 199, 26.7.1997, p. 32.

[6] OJ L 24, 30.1.1998, p. 1.

[7] OJ L 101, 1.4.1998, p. 24.

[8] OJ L 13, 19.1.2000, p. 12.

Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission(1),

Having regard to the opinion of the Economic and Social Committee(2),

Acting in accordance with the procedure laid down in Article 251 of the Treaty(3),

Whereas:

(1) Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)(4) lays down the objectives of a regulatory framework to cover electronic communications networks and services in the Community, including fixed and mobile telecommunications networks, cable television networks, networks used for terrestrial broadcasting, satellite networks and Internet networks, whether used for voice, fax, data or images. Such networks may have been authorised by Member States under Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive)(5) or have been authorised under previous regulatory measures. The provisions of this Directive apply to those networks that are used for the provision of publicly available electronic communications services. This Directive covers access and interconnection arrangements between service suppliers. Non-public networks do not have obligations under this Directive except where, in benefiting from access to public networks, they may be subject to conditions laid down by Member States.

(2) Services providing content such as the offer for sale of a package of sound or television broadcasting content are not covered by the common regulatory framework for electronic communications networks and services.

(3) The term "access" has a wide range of meanings, and it is therefore necessary to define precisely how that term is used in this Directive, without prejudice to how it may be used in other Community measures. An operator may own the underlying network or facilities or may rent some or all of them.

(4) Directive 95/47/EC of the European Parliament and of the Council of 24 October 1995 on the use of standards for the transmission of television signals(6) did not mandate any specific digital television transmission system or service requirement, and this opened up an opportunity for the market actors to take the initiative and develop suitable systems. Through the Digital Video Broadcasting Group, European market actors have developed a family of television transmission systems that have been adopted by broadcasters throughout the world. These transmissions systems have been standardised by the European Telecommunications Standards Institute (ETSI) and have become International Telecommunication Union recommendations. In relation to wide-screen digital television, the 16:9 aspect ratio is the reference format for wide-format television services and programmes, and is now established in Member States' markets as a result of Council Decision 93/424/EEC of 22 July 1993 on an action plan for the introduction of advanced television services in Europe(7).

(5) In an open and competitive market, there should be no restrictions that prevent undertakings from negotiating access and interconnection arrangements between themselves, in particular on cross-border agreements, subject to the competition rules of the Treaty. In the context of achieving a more efficient, truly pan-European market, with effective competition, more choice and competitive services to consumers, undertakings which receive requests for access or interconnection should in principle conclude such agreements on a commer-

cial basis, and negotiate in good faith.

(6) In markets where there continue to be large differences in negotiating power between undertakings, and where some undertakings rely on infrastructure provided by others for delivery of their services, it is appropriate to establish a framework to ensure that the market functions effectively. National regulatory authorities should have the power to secure, where commercial negotiation fails, adequate access and interconnection and interoperability of services in the interest of end-users. In particular, they may ensure end-to-end connectivity by imposing proportionate obligations on undertakings that control access to end-users. Control of means of access may entail ownership or control of the physical link to the end-user (either fixed or mobile), and/or the ability to change or withdraw the national number or numbers needed to access an end-user's network termination point. This would be the case for example if network operators were to restrict unreasonably end-user choice for access to Internet portals and services.

(7) National legal or administrative measures that link the terms and conditions for access or interconnection to the activities of the party seeking interconnection, and specifically to the degree of its investment in network infrastructure, and not to the interconnection or access services provided, may cause market distortion and may therefore not be compatible with competition rules.

(8) Network operators who control access to their own customers do so on the basis of unique numbers or addresses from a published numbering or addressing range. Other network operators need to be able to deliver traffic to those customers, and so need to be able to interconnect directly or indirectly to each other. The existing rights and obligations to negotiate interconnection should therefore be maintained. It is also appropriate to maintain the obligations formerly laid down in Directive 95/47/EC requiring fully digital electronic communications networks used for the distribution of television services and open to the public to be capable of distributing wide-screen television services and programmes, so that users are able to receive such programmes in the format in which they were transmitted.

(9) Interoperability is of benefit to end-users and is an important aim of this regulatory framework. Encouraging interoperability is one of the objectives for national regulatory authorities as set out in this framework, which also provides for the Commission to publish a list of standards and/or specifications covering the provision of services, technical interfaces and/or network functions, as the basis for encouraging harmonisation in electronic communications. Member States should encourage the use of published standards and/or specifications to the extent strictly necessary to ensure interoperability of services and to improve freedom of choice for users.

(10) Competition rules alone may not be sufficient to ensure cultural diversity and media pluralism in the area of digital television. Directive 95/47/EC provided an initial regulatory framework for the nascent digital television industry which should be maintained, including in particular the obligation to provide conditional access on fair, reasonable and non-discriminatory terms, in order to make sure that a wide variety of programming and services is available. Technological and market developments make it necessary to review these obligations on a regular basis, either by a Member State for its national market or the Commission for the Community, in particular to determine whether there is justification for extending obligations to new gateways, such as electronic programme guides (EPGs) and application program interfaces (APIs), to the extent that is necessary to ensure accessibility for end-users to specified digital broadcasting services. Member States may specify the digital broadcasting services to which access by end-users must be ensured by any legislative, regulatory or administrative means that they deem necessary.

(11) Member States may also permit their national regulatory authority to review obligations in relation to conditional access to digital broadcasting services in order to assess through a market analysis whether to withdraw or amend conditions for operators that do not have significant market power on the relevant market. Such withdrawal or amendment should not adversely affect access for end-users to such services or the prospects for effective competition.

(12) In order to ensure continuity of existing agreements and to avoid a legal vacuum, it is necessary to ensure that obligations for access and interconnection imposed under Articles 4, 6, 7, 8, 11, 12, and 14 of Directive 97/33/EC of the European Parliament and of the Council of 30 June 1997 on interconnection in telecommunications with regard to ensuring universal service

and interoperability through application of the principles of open network provision (ONP)(8), obligations on special access imposed under Article 16 of Directive 98/10/EC of the European Parliament and of the Council of 26 February 1998 on the application of open network provision (ONP) to voice telephony and on universal service for telecommunications in a competitive environment(9), and obligations concerning the provision of leased line transmission capacity under Council Directive 92/44/EEC of 5 June 1992 on the application of open network provision to leased lines(10), are initially carried over into the new regulatory framework, but are subject to immediate review in the light of prevailing market conditions. Such a review should also extend to those organisations covered by Regulation (EC) No 2887/2000 of the European Parliament and of the Council of 18 December 2000 on unbundled access to the local loop(11).

(13) The review should be carried out using an economic market analysis based on competition law methodology. The aim is to reduce ex ante sector specific rules progressively as competition in the market develops. However the procedure also takes account of transitional problems in the market such as those related to international roaming and of the possibility of new bottlenecks arising as a result of technological development, which may require ex ante regulation, for example in the area of broadband access networks. It may well be the case that competition develops at different speeds in different market segments and in different Member States, and national regulatory authorities should be able to relax regulatory obligations in those markets where competition is delivering the desired results. In order to ensure that market players in similar circumstances are treated in similar ways in different Member States, the Commission should be able to ensure harmonised application of the provisions of this Directive. National regulatory authorities and national authorities entrusted with the implementation of competition law should, where appropriate, coordinate their actions to ensure that the most appropriate remedy is applied. The Community and its Member States have entered into commitments on interconnection of telecommunications networks in the context of the World Trade Organisation agreement on basic telecommunications and these commitments need to be respected.

(14) Directive 97/33/EC laid down a range of obligations to be imposed on undertakings with significant market power, namely transparency, non-discrimination, accounting separation, access, and price control including cost orientation. This range of possible obligations should be maintained but, in addition, they should be established as a set of maximum obligations that can be applied to undertakings, in order to avoid over-regulation. Exceptionally, in order to comply with international commitments or Community law, it may be appropriate to impose obligations for access or interconnection on all market players, as is currently the case for conditional access systems for digital television services.

(15) The imposition of a specific obligation on an undertaking with significant market power does not require an additional market analysis but a justification that the obligation in question is appropriate and proportionate in relation to the nature of the problem identified.

(16) Transparency of terms and conditions for access and interconnection, including prices, serve to speed-up negotiation, avoid disputes and give confidence to market players that a service is not being provided on discriminatory terms. Openness and transparency of technical interfaces can be particularly important in ensuring interoperability. Where a national regulatory authority imposes obligations to make information public, it may also specify the manner in which the information is to be made available, covering for example the type of publication (paper and/or electronic) and whether or not it is free of charge, taking into account the nature and purpose of the information concerned.

(17) The principle of non-discrimination ensures that undertakings with market power do not distort competition, in particular where they are vertically integrated undertakings that supply services to undertakings with whom they compete on downstream markets.

(18) Accounting separation allows internal price transfers to be rendered visible, and allows national regulatory authorities to check compliance with obligations for non-discrimination where applicable. In this regard the Commission published Recommendation 98/322/EC of 8 April 1998 on interconnection in a liberalised telecommunications market (Part 2 - accounting separation and cost accounting)(12).

(19) Mandating access to network infrastructure can be justified as a means of increasing competition, but national regulatory authorities need to balance the rights of an infrastructure owner to exploit its infrastructure forits own benefit,

and the rights of other service providers to access facilities that are essential for the provision of competing services. Where obligations are imposed on operators that require them to meet reasonable requests for access to and use of networks elements and associated facilities, such requests should only be refused on the basis of objective criteria such as technical feasibility or the need to maintain network integrity. Where access is refused, the aggrieved party may submit the case to the dispute resolutions procedure referred to in Articles 20 and 21 of Directive 2002/21/EC (Framework Directive). An operator with mandated access obligations cannot be required to provide types of access which are not within its powers to provide. The imposition by national regulatory authorities of mandated access that increases competition in the short-term should not reduce incentives for competitors to invest in alternative facilities that will secure more competition in the long-term. The Commission has published a Notice on the application of the competition rules to access agreements in the telecommunications sector(13) which addresses these issues. National regulatory authorities may impose technical and operational conditions on the provider and/or beneficiaries of mandated access in accordance with Community law. In particular the imposition of technical standards should comply with Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules of Information Society Services(14).

(20) Price control may be necessary when market analysis in a particular market reveals inefficient competition. The regulatory intervention may be relatively light, such as an obligation that prices for carrier selection are reasonable as laid down in Directive 97/33/EC, or much heavier such as an obligation that prices are cost oriented to provide full justification for those prices where competition is not sufficiently strong to prevent excessive pricing. In particular, operators with significant market power should avoid a price squeeze whereby the difference between their retail prices and the interconnection prices charged to competitors who provide similar retail services is not adequate to ensure sustainable competition. When a national regulatory authority calculates costs incurred in establishing a service mandated under this Directive, it is appropriate to allow a reasonable return on the capital employed including appropriate labour and building costs, with the value of capital adjusted where necessary to reflect the current valuation of assets and efficiency of operations. The method of cost recovery should be appropriate to the circumstances taking account of the need to promote efficiency and sustainable competition and maximise consumer benefits.

(21) Where a national regulatory authority imposes obligations to implement a cost accounting system in order to support price controls, it may itself undertake an annual audit to ensure compliance with that cost accounting system, provided that it has the necessary qualified staff, or it may require the audit to be carried out by another qualified body, independent of the operator concerned.

(22) Publication of information by Member States will ensure that market players and potential market entrants understand their rights and obligations, and know where to find the relevant detailed information. Publication in the national gazette helps interested parties in other Member States to find the relevant information.

(23) In order to ensure that the pan-European electronic communications market is effective and efficient, the Commission should monitor and publish information on charges which contribute to determining prices to end-users.

(24) The development of the electronic communications market, with its associated infrastructure, could have adverse effects on the environment and the landscape. Member States should therefore monitor this process and, if necessary, take action to minimise any such effects by means of appropriate agreements and other arrangements with the relevant authorities.

(25) In order to determine the correct application of Community law, the Commission needs to know which undertakings have been designated as having significant market power and what obligations have been placed upon market players by national regulatory authorities. In addition to national publication of this information, it is therefore necessary for Member States to send this information to the Commission. Where Member States are required to send information to the Commission, this may be in electronic form, subject to appropriate authentication procedures being agreed.

(26) Given the pace of technological and market developments, the implementation of this Directive should be reviewed within three years of its

date of application to determine if it is meeting its objectives.

(27) The measures necessary for the implementation of this Directive should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission(15).

(28) Since the objectives of the proposed action, namely establishing a harmonised framework for the regulation of access to and interconnection of electronic communications networks and associated facilities, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of the action, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I
SCOPE, AIM AND DEFINITIONS

Article 1
Scope and aim

1. Within the framework set out in Directive 2002/21/EC (Framework Directive), this Directive harmonises the way in which Member States regulate access to, and interconnection of, electronic communications networks and associated facilities. The aim is to establish a regulatory framework, in accordance with internal market principles, for the relationships between suppliers of networks and services that will result in sustainable competition, interoperability of electronic communications services and consumer benefits.

2. This Directive establishes rights and obligations for operators and for undertakings seeking interconnection and/or access to their networks or associated facilities. It sets out objectives for national regulatory authorities with regard to access and interconnection, and lays down procedures to ensure that obligations imposed by national regulatory authorities are reviewed and, where appropriate, withdrawn once the desired objectives have been achieved. Access in this Directive does not refer to access by end-users.

Article 2
Definitions

For the purposes of this Directive the definitions set out in Article 2 of Directive 2002/21/EC (Framework Directive) shall apply.

The following definitions shall also apply:

(a) "access" means the making available of facilities and/or services, to another undertaking, under defined conditions, on either an exclusive or non-exclusive basis, for the purpose of providing electronic communications services. It covers inter alia: access to network elements and associated facilities, which may involve the connection of equipment, by fixed or non-fixed means (in particular this includes access to the local loop and to facilities and services necessary to provide services over the local loop), access to physical infrastructure including buildings, ducts and masts; access to relevant software systems including operational support systems, access to number translation or systems offering equivalent functionality, access to fixed and mobile networks, in particular for roaming, access to conditional access systems for digital television services; access to virtual network services;

(b) "interconnection" means the physical and logical linking of public communications networks used by the same or a different undertaking in order to allow the users of one undertaking to communicate with users of the same or another undertaking, or to access services provided by another undertaking. Services may be provided by the parties involved or other parties who have access to the network. Interconnection is a specific type of access implemented between public network operators;

(c) "operator" means an undertaking providing or authorised to provide a public communications network or an associated facility;

(d) "wide-screen television service" means a television service that consists wholly or partially of programmes produced and edited to be displayed in a full height wide-screen format. The 16:9 format is the reference format for wide-screen television services;

(e) "local loop" means the physical circuit connecting the network termination point at the

subscriber's premises to the main distribution frame or equivalent facility in the fixed public telephone network.

CHAPTER II
GENERAL PROVISIONS

Article 3
General framework for access and interconnection

1. Member States shall ensure that there are no restrictions which prevent undertakings in the same Member State or in different Member States from negotiating between themselves agreements on technical and commercial arrangements for access and/or interconnection, in accordance with Community law. The undertaking requesting access or interconnection does not need to be authorised to operate in the Member State where access or interconnection is requested, if it is not providing services and does not operate a network in that Member State.

2. Without prejudice to Article 31 of Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)(16), Member States shall not maintain legal or administrative measures which oblige operators, when granting access or interconnection, to offer different terms and conditions to different undertakings for equivalent services and/or imposing obligations that are not related to the actual access and interconnection services provided without prejudice to the conditions fixed in the Annex of Directive 2002/20/EC (Authorisation Directive).

Article 4
Rights and obligations for undertakings

1. Operators of public communications networks shall have a right and, when requested by other undertakings so authorised, an obligation to negotiate interconnection with each other for the purpose of providing publicly available electronic communications services, in order to ensure provision and interoperability of services throughout the Community. Operators shall offer access and interconnection to other undertakings on terms and conditions consistent with obligations imposed by the national regulatory authority pursuant to Articles 5, 6, 7 and 8.

2. Public electronic communications networks established for the distribution of digital television services shall be capable of distributing wide-screen television services and programmes. Network operators that receive and redistribute wide-screen television services or programmes shall maintain that wide-screen format.

3. Without prejudice to Article 11 of Directive 2002/20/EC (Authorisation Directive), Member States shall require that undertakings which acquire information from another undertaking before, during or after the process of negotiating access or interconnection arrangements use that information solely for the purpose for which it was supplied and respect at all times the confidentiality of information transmitted or stored. The received information shall not be passed on to any other party, in particular other departments, subsidiaries or partners, for whom such information could provide a competitive advantage.

Article 5
Powers and responsibilities of the national regulatory authorities with regard to access and interconnection

1. National regulatory authorities shall, acting in pursuit of the objectives set out in Article 8 of Directive 2002/21/EC (Framework Directive), encourage and where appropriate ensure, in accordance with the provisions of this Directive, adequate access and interconnection, and interoperability of services, exercising their responsibility in a way that promotes efficiency, sustainable competition, and gives the maximum benefit to end-users.

   In particular, without prejudice to measures that may be taken regarding undertakings with significant market power in accordance with Article 8, national regulatory authorities shall be able to impose:

   (a) to the extent that is necessary to ensure end-to-end connectivity, obligations on undertakings that control access to end-users, including in justified cases the obligation to interconnect their networks where this is not already the case;

   (b) to the extent that is necessary to ensure accessibility for end-users to digital radio and television broadcasting services specified by the Member State, obligations on operators to provide access to the other facilities re-

ferred to in Annex I, Part II on fair, reasonable and non-discriminatory terms.

2. When imposing obligations on an operator to provide access in accordance with Article 12, national regulatory authorities may lay down technical or operational conditions to be met by the provider and/or beneficiaries of such access, in accordance with Community law, where necessary to ensure normal operation of the network. Conditions that refer to implementation of specific technical standards or specifications shall respect Article 17 of Directive 2002/21/EC (Framework Directive).

3. Obligations and conditions imposed in accordance with paragraphs 1 and 2 shall be objective, transparent, proportionate and non-discriminatory, and shall be implemented in accordance with the procedures referred to in Articles 6 and 7 of Directive 2002/21/EC (Framework Directive).

4. With regard to access and interconnection, Member States shall ensure that the national regulatory authority is empowered to intervene at its own initiative where justified or, in the absence of agreement between undertakings, at the request of either of the parties involved, in order to secure the policy objectives of Article 8 of Directive 2002/21/EC (Framework Directive), in accordance with the provisions of this Directive and the procedures referred to in Articles 6 and 7, 20 and 21 of Directive 2002/21/EC (Framework Directive).

CHAPTER III
OBLIGATIONS ON OPERATORS AND MARKET REVIEW PROCEDURES

Article 6
Conditional access systems and other facilities

1. Member States shall ensure that, in relation to conditional access to digital television and radio services broadcast to viewers and listeners in the Community, irrespective of the means of transmission, the conditions laid down in Annex I, Part I apply.

2. In the light of market and technological developments, Annex I may be amended in accordance with the procedure referred to in Article 14(3).

3. Notwithstanding the provisions of paragraph 1, Member States may permit their national regulatory authority, as soon as possible after the entry into force of this Directive and periodically thereafter, to review the conditions applied in accordance with this Article, by undertaking a market analysis in accordance with the first paragraph of Article 16 of Directive 2002/21/EC (Framework Directive) to determine whether to maintain, amend or withdraw the conditions applied.

   Where, as a result of this market analysis, a national regulatory authority finds that one or more operators do not have significant market power on the relevant market, it may amend or withdraw the conditions with respect to those operators, in accordance with the procedures referred to in Articles 6 and 7 of Directive 2002/21/EC (Framework Directive), only to the extent that:

   (a) accessibility for end-users to radio and television broadcasts and broadcasting channels and services specified in accordance with Article 31 of Directive 2002/22/EC (Universal Service Directive) would not be adversely affected by such amendment or withdrawal, and

   (b) the prospects for effective competition in the markets for:

      (i) retail digital television and radio broadcasting services, and

      (ii) conditional access systems and other associated facilities,

   would not be adversely affected by such amendment or withdrawal.

   An appropriate period of notice shall be given to parties affected by such amendment or withdrawal of conditions.

4. Conditions applied in accordance with this Article are without prejudice to the ability of Member States to impose obligations in relation to the presentational aspect of electronic programme guides and similar listing and navigation facilities.

Article 7
Review of former obligations for access and interconnection

1. Member States shall maintain all obligations on undertakings providing public communications networks and/or services concerning access and interconnection that were in force

prior to the date of entry into force of this Directive under Articles 4, 6, 7, 8, 11, 12, and 14 of Directive 97/33/EC, Article 16 of Directive 98/10/EC, and Articles 7 and 8 of Directive 92/44/EC, until such time as these obligations have been reviewed and a determination made in accordance with paragraph 3.

2. The Commission will indicate relevant markets for the obligations referred to in paragraph 1 in the initial recommendation on relevant product and service markets and the Decision identifying transnational markets to be adopted in accordance with Article 15 of Directive 2002/21/EC (Framework Directive).

3. Member States shall ensure that, as soon as possible after the entry into force of this Directive, and periodically thereafter, national regulatory authorities undertake a market analysis, in accordance with Article 16 of Directive 2002/21/EC (Framework Directive) to determine whether to maintain, amend or withdraw these obligations. An appropriate period of notice shall be given to parties affected by such amendment or withdrawal of obligations.

Article 8
Imposition, amendment or withdrawal of obligations

1. Member States shall ensure that national regulatory authorities are empowered to impose the obligations identified in Articles 9 to 13.

2. Where an operator is designated as having significant market power on a specific market as a result of a market analysis carried out in accordance with Article 16 of Directive 2002/21/EC (Framework Directive), national regulatory authorities shall impose the obligations set out in Articles 9 to 13 of this Directive as appropriate.

3. Without prejudice to:

   - the provisions of Articles 5(1), 5(2) and 6,
   - the provisions of Articles 12 and 13 of Directive 2002/21/EC (Framework Directive), Condition 7 in Part B of the Annex to Directive 2002/20/EC (Authorisation Directive) as applied by virtue of Article 6(1) of that Directive, Articles 27, 28 and 30 of Directive 2002/22/EC (Universal Service Directive) and the relevant provisions of Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(17) containing obligations on undertakings other than those designated as having significant market power, or
   - the need to comply with international commitments,

   national regulatory authorities shall not impose the obligations set out in Articles 9 to 13 on operators that have not been designated in accordance with paragraph 2.

   In exceptional circumstances, when a national regulatory authority intends to impose on operators with significant market power other obligations for access or interconnection than those set out in Articles 9 to 13 in this Directive it shall submit this request to the Commission. The Commission, acting in accordance with Article 14(2), shall take a decision authorising or preventing the national regulatory authority from taking such measures.

4. Obligations imposed in accordance with this Article shall be based on the nature of the problem identified, proportionate and justified in the light of the objectives laid down in Article 8 of Directive 2002/21/EC (Framework Directive). Such obligations shall only be imposed following consultation in accordance with Articles 6 and 7 of that Directive.

5. In relation to the third indent of the first subparagraph of paragraph 3, national regulatory authorities shall notify decisions to impose, amend or withdraw obligations on market players to the Commission, in accordance with the procedure referred to in Article 7 of Directive 2002/21/EC (Framework Directive).

Article 9
Obligation of transparency

1. National regulatory authorities may, in accordance with the provisions of Article 8, impose obligations for transparency in relation to interconnection and/or access, requiring operators to make public specified information, such as accounting information, technical specifications, network characteristics, terms and conditions for supply and use, and prices.

2. In particular where an operator has obligations of non-discrimination, national regulatory authorities may require that operator to publish a reference offer, which shall be sufficiently unbundled to ensure that undertakings are not required to pay for facilities which are not

necessary for the service requested, giving a description of the relevant offerings broken down into components according to market needs, and the associated terms and conditions including prices. The national regulatory authority shall, inter alia, be able to impose changes to reference offers to give effect to obligations imposed under this Directive.

3. National regulatory authorities may specify the precise information to be made available, the level of detail required and the manner of publication.

4. Notwithstanding paragraph 3, where an operator has obligations under Article 12 concerning unbundled access to the twisted metallic pair local loop, national regulatory authorities shall ensure the publication of a reference offer containing at least the elements set out in Annex II.

5. In the light of market and technological developments, Annex II may be amended in accordance with the procedure referred to in Article 14(3).

Article 10
Obligation of non-discrimination

1. A national regulatory authority may, in accordance with the provisions of Article 8, impose obligations of non-discrimination, in relation to interconnection and/or access.

2. Obligations of non-discrimination shall ensure, in particular, that the operator applies equivalent conditions in equivalent circumstances to other undertakings providing equivalent services, and provides services and information to others under the same conditions and of the same quality as it provides for its own services, or those of it subsidiaries or partners.

Article 11
Obligation of accounting separation

1. A national regulatory authority may, in accordance with the provisions of Article 8, impose obligations for accounting separation in relation to specified activities related to interconnection and/or access.

   In particular, a national regulatory authority may require a vertically integrated company to make transparent its wholesale prices and its internal transfer prices inter alia to ensure compliance where there is a requirement for non-discrimination under Article 10 or, where necessary, to prevent unfair cross-subsidy. National regulatory authorities may specify the format and accounting methodology to be used.

2. Without prejudice to Article 5 of Directive 2002/21/EC (Framework Directive), to facilitate the verification of compliance with obligations of transparency and non-discrimination, national regulatory authorities shall have the power to require that accounting records, including data on revenues received from third parties, are provided on request. National regulatory authorities may publish such information as would contribute to an open and competitive market, while respecting national and Community rules on commercial confidentiality.

Article 12
Obligations of access to, and use of, specific network facilities

1. A national regulatory authority may, in accordance with the provisions of Article 8, impose obligations on operators to meet reasonable requests for access to, and use of, specific network elements and associated facilities, inter alia in situations where the national regulatory authority considers that denial of access or unreasonable terms and conditions having a similar effect would hinder the emergence of a sustainable competitive market at the retail level, or would not be in the end-user's interest.

   Operators may be required inter alia:

   (a) to give third parties access to specified network elements and/or facilities, including unbundled access to the local loop;

   (b) to negotiate in good faith with undertakings requesting access;

   (c) not to withdraw access to facilities already granted;

   (d) to provide specified services on a wholesale basis for resale by third parties;

   (e) to grant open access to technical interfaces, protocols or other key technologies that are indispensable for the interoperability of services or virtual network services;

   (f) to provide co-location or other forms of facility sharing, including duct, building or mast sharing;

   (g) to provide specified services needed to ensure interoperability of end-to-end services to users, including facilities for intelligent

network services or roaming on mobile networks;

(h) to provide access to operational support systems or similar software systems necessary to ensure fair competition in the provision of services;

(i) to interconnect networks or network facilities.

National regulatory authorities may attach to those obligations conditions covering fairness, reasonableness and timeliness.

2. When national regulatory authorities are considering whether to impose the obligations referred in paragraph 1, and in particular when assessing whether such obligations would be proportionate to the objectives set out in Article 8 of Directive 2002/21/EC (Framework Directive), they shall take account in particular of the following factors:

(a) the technical and economic viability of using or installing competing facilities, in the light of the rate of market development, taking into account the nature and type of interconnection and access involved;

(b) the feasibility of providing the access proposed, in relation to the capacity available;

(c) the initial investment by the facility owner, bearing in mind the risks involved in making the investment;

(d) the need to safeguard competition in the long term;

(e) where appropriate, any relevant intellectual property rights;

(f) the provision of pan-European services.

Article 13
Price control and cost accounting obligations

1. A national regulatory authority may, in accordance with the provisions of Article 8, impose obligations relating to cost recovery and price controls, including obligations for cost orientation of prices and obligations concerning cost accounting systems, for the provision of specific types of interconnection and/or access, in situations where a market analysis indicates that a lack of effective competition means that the operator concerned might sustain prices at an excessively high level, or apply a price squeeze, to the detriment of end-users. National regulatory authorities shall take into account the investment made by the operator and allow him a reasonable rate of return on adequate capital employed, taking into account the risks involved.

2. National regulatory authorities shall ensure that any cost recovery mechanism or pricing methodology that is mandated serves to promote efficiency and sustainable competition and maximise consumer benefits. In this regard national regulatory authorities may also take account of prices available in comparable competitive markets.

3. Where an operator has an obligation regarding the cost orientation of its prices, the burden of proof that charges are derived from costs including a reasonable rate of return on investment shall lie with the operator concerned. For the purpose of calculating the cost of efficient provision of services, national regulatory authorities may use cost accounting methods independent of those used by the undertaking. National regulatory authorities may require an operator to provide full justification for its prices, and may, where appropriate, require prices to be adjusted.

4. National regulatory authorities shall ensure that, where implementation of a cost accounting system is mandated in order to support price controls, a description of the cost accounting system is made publicly available, showing at least the main categories under which costs are grouped and the rules used for the allocation of costs. Compliance with the cost accounting system shall be verified by a qualified independent body. A statement concerning compliance shall be published annually.

CHAPTER IV
PROCEDURAL PROVISIONS

Article 14
Committee

1. The Commission shall be assisted by the Communications Committee set up by Article 22 of Directive 2002/21/EC (Framework Directive).

2. Where reference is made to this paragraph, Articles 3 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

3. Where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall

apply, having regard to the provisions of Article 8 thereof.

The period laid down in Article 5(6) of Decision 1999/468/EC shall be set at three months.

4. The Committee shall adopt its rules of procedure.

Article 15
Publication of, and access to, information

1. Member States shall ensure that the specific obligations imposed on undertakings under this Directive are published and that the specific product/service and geographical markets are identified. They shall ensure that up-to-date information, provided that the information is not confidential and, in particular, does not comprise business secrets, is made publicly available in a manner that guarantees all interested parties easy access to that information.

2. Member States shall send to the Commission a copy of all such information published. The Commission shall make this information available in a readily accessible form, and shall distribute the information to the Communications Committee as appropriate.

Article 16
Notification

1. Member States shall notify to the Commission by at the latest the date of application referred to in Article 18(1) second subparagraph the national regulatory authorities responsible for the tasks set out in this Directive.

2. National regulatory authorities shall notify to the Commission the names of operators deemed to have significant market power for the purposes of this Directive, and the obligations imposed upon them under this Directive. Any changes affecting the obligations imposed upon undertakings or of the undertakings affected under the provisions of this Directive shall be notified to the Commission without delay.

Article 17
Review procedures

The Commission shall periodically review the functioning of this Directive and report to the European Parliament and to the Council, on the first occasion not later than three years after the date of application referred to in Article 18(1), second subparagraph. For this purpose, the Commission may request from the Member States information, which shall be supplied without undue delay.

Article 18
Transposition

1. Member States shall adopt and publish the laws, regulations and administrative provisions necessary to comply with this Directive by not later than 24 July 2003. They shall forthwith inform the Commission thereof.

They shall apply those measures from 25 July 2003.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive and of any subsequent amendments to those provisions.

Article 19
Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 20
Addressees

This Directive is addressed to the Member States.

Done at Brussels, 7 March 2002.
For the European Parliament
The President P. Cox
For the Council
The President J. C. Aparicio

[1] OJ C 365 E, 19.12.2000, p. 215 and OJ C 270 E, 25.9.2001, p. 161.

[2] OJ C 123, 25.4.2001, p. 50.

[3] Opinion of the European Parliament of 1 March 2001 (OJ C 277, 1.10.2001, p. 72), Council Common Position of 17 September 2001 (OJ C 337, 30.11.2001, p. 1) and Decision of the European Parliament of 12 December 2001 (not yet published in the Official Journal). Council Decision of 14 February 2002.

[4] See page 33 of this Official Journal.

[5] See page 21 of this Official Journal.

[6] OJ L 281, 23.11.1995, p. 51.

[7] OJ L 196, 5.8.1993, p. 48.

[8] OJ L 199, 26.7.1997, p. 32. Directive as last amended by Directive 98/61/EC (OJ L 268, 3.10.1998, p. 37).

[9] OJ L 101, 1.4.1998, p. 24.

[10] OJ L 165, 19.6.1992, p. 27. Directive as last amended by Commission Decision No 98/80/EC (OJ L 14, 20.1.1998, p. 27).

[11] OJ L 366, 30.12.2000, p. 4.

[12] OJ L 141, 13.5.1998, p. 6.

[13] OJ C 265, 22.8.1998, p. 2.

[14] OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).

[15] OJ L 184, 17.7.1999, p. 23.

[16] See page 51 of this Official Journal.

[17] OJ L 24, 30.1.1998, p. 1.

ANNEX I

CONDITIONS FOR ACCESS TO DIGITAL TELEVISION AND RADIO SERVICES BROADCAST TO VIEWERS AND LISTENERS IN THE COMMUNITY

Part I: Conditions for conditional access systems to be applied in accordance with Article 6(1)

In relation to conditional access to digital television and radio services broadcast to viewers and listeners in the Community, irrespective of the means of transmission, Member States must ensure in accordance with Article 6 that the following conditions apply:

(a) conditional access systems operated on the market in the Community are to have the necessary technical capability for cost-effective transcontrol allowing the possibility for full control by network operators at local or regional level of the services using such conditional access systems;

(b) all operators of conditional access services, irrespective of the means of transmission, who provide access services to digital television and radio services and whose access services broadcasters depend on to reach any group of potential viewers or listeners are to:

- offer to all broadcasters, on a fair, reasonable and non-discriminatory basis compatible with Community competition law, technical services enabling the broadcasters' digitally-transmitted services to be received by viewers or listeners authorised by means of decoders administered by the service operators, and comply with Community competition law,
- keep separate financial accounts regarding their activity as conditional access providers.

(c) when granting licences to manufacturers of consumer equipment, holders of industrial property rights to conditional access products and systems are to ensure that this is done on fair, reasonable and non-discriminatory terms. Taking into account technical and commercial factors, holders of rights are not to subject the granting of licences to conditions prohibiting, deterring or discouraging the inclusion in the same product of:

- a common interface allowing connection with several other access systems, or
- means specific to another access system, provided that the licensee complies with the relevant and reasonable conditions ensuring, as far as he is concerned, the security of transactions of conditional access system operators.

Part II: Other facilities to which conditions may be applied under Article 5(1)(b)

(a) Access to application program interfaces (APIs);

(b) Access to electronic programme guides (EPGs).

ANNEX II

MINIMUM LIST OF ITEMS TO BE INCLUDED IN A REFERENCE OFFER FOR UNBUNDLED ACCESS TO THE TWISTED METALLIC PAIR LOCAL LOOP TO BE PUBLISHED BY NOTIFIED OPERATORS

For the purposes of this Annex the following definitions apply:

(a) "local sub-loop" means a partial local loop connecting the network termination point at the subscriber's premises to a concentration point or a specified intermediate access point in the fixed public telephone network;

(b) "unbundled access to the local loop" means full unbundled access to the local loop and shared access to the local loop; it does not entail a change in ownership of the local loop;

(c) "full unbundled access to the local loop" means the provision to a beneficiary of access to the local loop or local sub-loop of the notified operator authorising the use of the full frequency spectrum of the twisted metallic pair;

(d) "shared access to the local loop" means the provision to a beneficiary of access to the local loop or local sub-loop of the notified operator, authorising the use of the non-voice band frequency spectrum of the twisted metallic pair; the local loop continues to be used by the notified operator to provide the telephone service to the public;

A. Conditions for unbundled access to the local loop

1. Network elements to which access is offered covering in particular the following elements:

   (a) access to local loops;

   (b) access to non-voice band frequency spectrum of a local loop, in the case of shared access to the local loop;

2. Information concerning the locations of physical access sites(1), availability of local loops in specific parts of the access network;

3. Technical conditions related to access and use of local loops, including the technical characteristics of the twisted metallic pair in the local loop;

4. Ordering and provisioning procedures, usage restrictions.

B. Co-location services

1. Information on the notified operator's relevant sites(2).

2. Co-location options at the sites indicated under point 1 (including physical co-location and, as appropriate, distant co-location and virtual co-location).

3. Equipment characteristics: restrictions, if any, on equipment that can be co-located.

4. Security issues: measures put in place by notified operators to ensure the security of their locations.

5. Access conditions for staff of competitive operators.

6. Safety standards.

7. Rules for the allocation of space where co-location space is limited.

8. Conditions for beneficiaries to inspect the locations at which physical co-location is available, or sites where co-location has been refused on grounds of lack of capacity.

C. Information systems

Conditions for access to notified operator's operational support systems, information systems or databases for pre-ordering, provisioning, ordering, maintenance and repair requests and billing.

D. Supply conditions

1. Lead time for responding to requests for supply of services and facilities; service level agreements, fault resolution, procedures to return to a normal level of service and quality of service parameters.

2. Standard contract terms, including, where appropriate, compensation provided for failure to meet lead times.

3. Prices or pricing formulae for each feature, function and facility listed above.

(1) Availability of this information may be restricted to interested parties only, in order to avoid public security concerns.

(2) Availability of this information may be restricted to interested parties only, in order to avoid public security concerns.

Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission(1),

Having regard to the opinion of the Economic and Social Committee(2),

Acting in accordance with the procedure laid down in Article 251 of the Treaty(3),

Whereas:

(1) The outcome of the public consultation on the 1999 review of the regulatory framework for electronic communications, as reflected in the Commission communication of 26 April 2000, and the findings reported by the Commission in its communications on the fifth and sixth reports on the implementation of the telecommunications regulatory package, has confirmed the need for a more harmonised and less onerous market access regulation for electronic communications networks and services throughout the Community.

(2) Convergence between different electronic communications networks and services and their technologies requires the establishment of an authorisation system covering all comparable services in a similar way regardless of the technologies used.

(3) The objective of this Directive is to create a legal framework to ensure the freedom to provide electronic communications networks and services, subject only to the conditions laid down in this Directive and to any restrictions in conformity with Article 46(1) of the Treaty, in particular measures regarding public policy, public security and public health.

(4) This Directive covers authorisation of all electronic communications networks and services whether they are provided to the public or not. This is important to ensure that both categories of providers may benefit from objective, transparent, non-discriminatory and proportionate rights, conditions and procedures.

(5) This Directive only applies to the granting of rights to use radio frequencies where such use involves the provision of an electronic communications network or service, normally for remuneration. The self-use of radio terminal equipment, based on the non-exclusive use of specific radio frequencies by a user and not related to an economic activity, such as use of a citizen's band by radio amateurs, does not consist of the provision of an electronic communications network or service and is therefore not covered by this Directive. Such use is covered by the Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity(4).

(6) Provisions regarding the free movement of conditional access systems and the free provision of protected services based on such systems are laid down in Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access(5). The authorisation of such systems and services therefore does not need to be covered by this Directive.

(7) The least onerous authorisation system possible should be used to allow the provision of electronic communications networks and services in order to stimulate the development of new electronic communications services and pan-European communications networks and services and to allow service providers and consumers to benefit from the economies of scale of the single market.

(8) Those aims can be best achieved by general authorisation of all electronic communications networks and services without requiring any explicit decision or administrative act by the national regulatory authority and by limiting any procedural requirements to notification only. Where Member States require notification by providers of electronic communication networks or services when they start their activities, they may also require proof of such notification

having been made by means of any legally recognised postal or electronic acknowledgement of receipt of the notification. Such acknowledgement should in any case not consist of or require an administrative act by the national regulatory authority to which the notification must be made.

(9) It is necessary to include the rights and obligations of undertakings under general authorisations explicitly in such authorisations in order to ensure a level playing field throughout the Community and to facilitate cross-border negotiation of interconnection between public communications networks.

(10) The general authorisation entitles undertakings providing electronic communications networks and services to the public to negotiate interconnection under the conditions of Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communication networks and associated facilities (Access Directive)(6). Undertakings providing electronic communications networks and services other than to the public can negotiate interconnection on commercial terms.

(11) The granting of specific rights may continue to be necessary for the use of radio frequencies and numbers, including short codes, from the national numbering plan. Rights to numbers may also be allocated from a European numbering plan, including for example the virtual country code "3883" which has been attributed to member countries of the European Conference of Post and Telecommunications (CEPT). Those rights of use should not be restricted except where this is unavoidable in view of the scarcity of radio frequencies and the need to ensure the efficient use thereof.

(12) This Directive does not prejudice whether radio frequencies are assigned directly to providers of electronic communication networks or services or to entities that use these networks or services. Such entities may be radio or television broadcast content providers. Without prejudice to specific criteria and procedures adopted by Member States to grant rights of use for radio frequencies to providers of radio or television broadcast content services, to pursue general interest objectives in conformity with Community law, the procedure for assignment of radio frequencies should in any event be objective, transparent, non-discriminatory and proportionate. In accordance with case law of the Court of Justice, any national restrictions on the rights guaranteed by Article 49 of the Treaty should be objectively justified, proportionate and not exceed what is necessary to achieve general interest objectives as defined by Member States in conformity with Community law. The responsibility for compliance with the conditions attached to the right to use a radio frequency and the relevant conditions attached to the general authorisation should in any case lie with the undertaking to whom the right of use for the radio frequency has been granted.

(13) As part of the application procedure for granting rights to use a radio frequency, Member States may verify whether the applicant will be able to comply with the conditions attached to such rights. For this purpose the applicant may be requested to submit the necessary information to prove his ability to comply with these conditions. Where such information is not provided, the application for the right to use a radio frequency may be rejected.

(14) Member States are neither obliged to grant nor prevented from granting rights to use numbers from the national numbering plan or rights to install facilities to undertakings other than providers of electronic communications networks or services.

(15) The conditions, which may be attached to the general authorisation and to the specific rights of use, should be limited to what is strictly necessary to ensure compliance with requirements and obligations under Community law and national law in accordance with Community law.

(16) In the case of electronic communications networks and services not provided to the public it is appropriate to impose fewer and lighter conditions than are justified for electronic communications networks and services provided to the public.

(17) Specific obligations which may be imposed on providers of electronic communications networks and services in accordance with Community law by virtue of their significant market power as defined in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)(7) should be imposed separately from the general rights and obligations under the general authorisation.

(18) The general authorisation should only contain conditions which are specific to the electronic

communications sector. It should not be made subject to conditions which are already applicable by virtue of other existing national law which is not specific to the electronic communications sector. Nevertheless, the national regulatory authorities may inform network operators and service providers about other legislation concerning their business, for instance through references on their websites.

(19) The requirement to publish decisions on the granting of rights to use frequencies or numbers may be fulfilled by making these decisions publicly accessible via a website.

(20) The same undertaking, for example a cable operator, can offer both an electronic communications service, such as the conveyance of television signals, and services not covered under this Directive, such as the commercialisation of an offer of sound or television broadcasting content services, and therefore additional obligations can be imposed on this undertaking in relation to its activity as a content provider or distributor, according to provisions other than those of this Directive, without prejudice to the list of conditions laid in the Annex to this Directive.

(21) When granting rights of use for radio frequencies, numbers or rights to install facilities, the relevant authorities may inform the undertakings to whom they grant such rights of the relevant conditions in the general authorisation.

(22) Where the demand for radio frequencies in a specific range exceeds their availability, appropriate and transparent procedures should be followed for the assignment of such frequencies in order to avoid any discrimination and optimise use of those scarce resources.

(23) National regulatory authorities should ensure, in establishing criteria for competitive or comparative selection procedures, that the objectives in Article 8 of Directive 2002/21/EC (Framework Directive) are met. It would therefore not be contrary to this Directive if the application of objective, non-discriminatory and proportionate selection criteria to promote the development of competition would have the effect of excluding certain undertakings from a competitive or comparative selection procedure for a particular radio frequency.

(24) Where the harmonised assignment of radio frequencies to particular undertakings has been agreed at European level, Member States should strictly implement such agreements in the granting of rights of use of radio frequencies from the national frequency usage plan.

(25) Providers of electronic communications networks and services may need a confirmation of their rights under the general authorisation with respect to interconnection and rights of way, in particular to facilitate negotiations with other, regional or local, levels of government or with service providers in other Member States. For this purpose the national regulatory authorities should provide declarations to undertakings either upon request or alternatively as an automatic response to a notification under the general authorisation. Such declarations should not by themselves constitute entitlements to rights nor should any rights under the general authorisation or rights of use or the exercise of such rights depend upon a declaration.

(26) Where undertakings find that their applications for rights to install facilities have not been dealt with in accordance with the principles set out in Directive 2002/21/EC (Framework Directive) or where such decisions are unduly delayed, they should have the right to appeal against decisions or delays in such decisions in accordance with that Directive.

(27) The penalties for non-compliance with conditions under the general authorisation should be commensurate with the infringement. Save in exceptional circumstances, it would not be proportionate to suspend or withdraw the right to provide electronic communications services or the right to use radio frequencies or numbers where an undertaking did not comply with one or more of the conditions under the general authorisation. This is without prejudice to urgent measures which the relevant authorities of the Member States may need to take in case of serious threats to public safety, security or health or to economic and operational interests of other undertakings. This Directive should also be without prejudice to any claims between undertakings for compensation for damages under national law.

(28) Subjecting service providers to reporting and information obligations can be cumbersome, both for the undertaking and for the national regulatory authority concerned. Such obligations should therefore be proportionate, objectively justified and limited to what is strictly necessary. It is not necessary to require systematic and regular proof of compliance with all conditions under the general authorisation or attached to rights of use. Undertakings have a

right to know the purposes for which the information they should provide will be used. The provision of information should not be a condition for market access. For statistical purposes a notification may be required from providers of electronic communication networks or services when they cease activities.

(29) This Directive should be without prejudice to Member States' obligations to provide any information necessary for the defence of Community interests within the context of international agreements. This Directive should also be without prejudice to any reporting obligations under legislation which is not specific to the electronic communications sector such as competition law.

(30) Administrative charges may be imposed on providers of electronic communications services in order to finance the activities of the national regulatory authority in managing the authorisation system and for the granting of rights of use. Such charges should be limited to cover the actual administrative costs for those activities. For this purpose transparency should be created in the income and expenditure of national regulatory authorities by means of annual reporting about the total sum of charges collected and the administrative costs incurred. This will allow undertakings to verify that administrative costs and charges are in balance.

(31) Systems for administrative charges should not distort competition or create barriers for entry into the market. With a general authorisation system it will no longer be possible to attribute administrative costs and hence charges to individual undertakings except for the granting of rights to use numbers, radio frequencies and for rights to install facilities. Any applicable administrative charges should be in line with the principles of a general authorisation system. An example of a fair, simple and transparent alternative for these charge attribution criteria could be a turnover related distribution key. Where administrative charges are very low, flat rate charges, or charges combining a flat rate basis with a turnover related element could also be appropriate.

(32) In addition to administrative charges, usage fees may be levied for the use of radio frequencies and numbers as an instrument to ensure the optimal use of such resources. Such fees should not hinder the development of innovative services and competition in the market. This Directive is without prejudice to the purpose for which fees for rights of use are employed. Such fees may for instance be used to finance activities of national regulatory authorities that cannot be covered by administrative charges. Where, in the case of competitive or comparative selection procedures, fees for rights of use for radio frequencies consist entirely or partly of a one-off amount, payment arrangements should ensure that such fees do not in practice lead to selection on the basis of criteria unrelated to the objective of ensuring optimal use of radio frequencies. The Commission may publish on a regular basis benchmark studies with regard to best practices for the assignment of radio frequencies, the assignment of numbers or the granting of rights of way.

(33) Member States may need to amend rights, conditions, procedures, charges and fees relating to general authorisations and rights of use where this is objectively justified. Such changes should be duly notified to all interested parties in good time, giving them adequate opportunity to express their views on any such amendments.

(34) The objective of transparency requires that service providers, consumers and other interested parties have easy access to any information regarding rights, conditions, procedures, charges, fees and decisions concerning the provision of electronic communications services, rights of use of radio frequencies and numbers, rights to install facilities, national frequency usage plans and national numbering plans. The national regulatory authorities have an important task in providing such information and keeping it up to date. Where such rights are administered by other levels of government the national regulatory authorities should endeavour to create a user-friendly instrument for access to information regarding such rights.

(35) The proper functioning of the single market on the basis of the national authorisation regimes under this Directive should be monitored by the Commission.

(36) In order to arrive at a single date of application of all elements of the new regulatory framework for the electronic communications sector, it is important that the process of national transposition of this Directive and of alignment of the existing licences with the new rules take place in parallel. However, in specific cases where the replacement of authorisations existing on the date of entry into force of this Directive by the general authorisation and the individual rights of use in accordance with this Directive would

lead to an increase in the obligations for service providers operating under an existing authorisation or to a reduction of their rights, Member States may avail themselves of an additional nine months after the date of application of this Directive for alignment of such licences, unless this would have a negative effect on the rights and obligations of other undertakings.

(37) There may be circumstances under which the abolition of an authorisation condition regarding access to electronic communications networks would create serious hardship for one or more undertakings that have benefited from the condition. In such cases further transitional arrangements may be granted by the Commission, upon request by a Member State.

(38) Since the objectives of the proposed action, namely the harmonisation and simplification of electronic communications rules and conditions for the authorisation of networks and services cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of the action, be better achieved at Community level, the Community may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary for those objectives,

HAVE ADOPTED THIS DIRECTIVE:

Article 1
Objective and scope

1. The aim of this Directive is to implement an internal market in electronic communications networks and services through the harmonisation and simplification of authorisation rules and conditions in order to facilitate their provision throughout the Community.

2. This Directive shall apply to authorisations for the provision of electronic communications networks and services.

Article 2
Definitions

1. For the purposes of this Directive, the definitions set out in Article 2 of Directive 2002/21/EC (Framework Directive) shall apply.

2. The following definitions shall also apply:

(a) "general authorisation" means a legal framework established by the Member State ensuring rights for the provision of electronic communications networks or services and laying down sector specific obligations that may apply to all or to specific types of electronic communications networks and services, in accordance with this Directive;

(b) "harmful interference" means interference which endangers the functioning of a radionavigation service or of other safety services or which otherwise seriously degrades, obstructs or repeatedly interrupts a radiocommunications service operating in accordance with the applicable Community or national regulations.

Article 3
General authorisation of electronic communications networks and services

1. Member States shall ensure the freedom to provide electronic communications networks and services, subject to the conditions set out in this Directive. To this end, Member States shall not prevent an undertaking from providing electronic communications networks or services, except where this is necessary for the reasons set out in Article 46(1) of the Treaty.

2. The provision of electronic communications networks or the provision of electronic communications services may, without prejudice to the specific obligations referred to in Article 6(2) or rights of use referred to in Article 5, only be subject to a general authorisation. The undertaking concerned may be required to submit a notification but may not be required to obtain an explicit decision or any other administrative act by the national regulatory authority before exercising the rights stemming from the authorisation. Upon notification, when required, an undertaking may begin activity, where necessary subject to the provisions on rights of use in Articles 5, 6 and 7.

3. The notification referred to in paragraph 2 shall not entail more than a declaration by a legal or natural person to the national regulatory authority of the intention to commence the provision of electronic communication networks or services and the submission of the minimal information which is required to allow the national regulatory authority to keep a register or list of providers of electronic communications networks and services. This information must be limited to what is necessary for the identi-

fication of the provider, such as company registration numbers, and the provider's contact persons, the provider's address, a short description of the network or service, and an estimated date for starting the activity.

Article 4
Minimum list of rights derived from the general authorisation

1. Undertakings authorised pursuant to Article 3, shall have the right to:

   (a) provide electronic communications networks and services;

   (b) have their application for the necessary rights to install facilities considered in accordance with Article 11 of Directive 2002/21/EC (Framework Directive).

2. When such undertakings provide electronic communications networks or services to the public the general authorisation shall also give them the right to:

   (a) negotiate interconnection with and where applicable obtain access to or interconnection from other providers of publicly available communications networks and services covered by a general authorisation anywhere in the Community under the conditions of and in accordance with Directive 2002/19/EC (Access Directive);

   (b) be given an opportunity to be designated to provide different elements of a universal service and/or to cover different parts of the national territory in accordance with Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)(8).

Article 5
Rights of use for radio frequencies and numbers

1. Member States shall, where possible, in particular where the risk of harmful interference is negligible, not make the use of radio frequencies subject to the grant of individual rights of use but shall include the conditions for usage of such radio frequencies in the general authorisation.

2. Where it is necessary to grant individual rights of use for radio frequencies and numbers, Member States shall grant such rights, upon request, to any undertaking providing or using networks or services under the general authorisation, subject to the provisions of Articles 6, 7 and 11(1)(c) of this Directive and any other rules ensuring the efficient use of those resources in accordance with Directive 2002/21/EC (Framework Directive).

   Without prejudice to specific criteria and procedures adopted by Member States to grant rights of use of radio frequencies to providers of radio or television broadcast content services with a view to pursuing general interest objectives in conformity with Community law, such rights of use shall be granted through open, transparent and non-discriminatory procedures. When granting rights of use, Member States shall specify whether those rights can be transferred at the initiative of the right holder, and under which conditions, in the case of radio frequencies, in accordance with Article 9 of Directive 2002/21/EC (Framework Directive). Where Member States grant rights of use for a limited period of time, the duration shall be appropriate for the service concerned.

3. Decisions on rights of use shall be taken, communicated and made public as soon as possible after receipt of the complete application by the national regulatory authority, within three weeks in the case of numbers that have been allocated for specific purposes within the national numbering plan and within six weeks in the case of radio frequencies that have been allocated for specific purposes within the national frequency plan. The latter time limit shall be without prejudice to any applicable international agreements relating to the use of radio frequencies or of orbital positions.

4. Where it has been decided, after consultation with interested parties in accordance with Article 6 of Directive 2002/21/EC (Framework Directive), that rights for use of numbers of exceptional economic value are to be granted through competitive or comparative selection procedures, Member States may extend the maximum period of three weeks by up to three weeks.

   With regard to competitive or comparative selection procedures for radio frequencies Article 7 shall apply.

5. Member States shall not limit the number of rights of use to be granted except where this is necessary to ensure the efficient use of radio frequencies in accordance with Article 7.

Article 6
Conditions attached to the general authorisation and to the rights of use for radio frequencies and for numbers, and specific obligations

1. The general authorisation for the provision of electronic communications networks or services and the rights of use for radio frequencies and rights of use for numbers may be subject only to the conditions listed respectively in parts A, B and C of the Annex. Such conditions shall be objectively justified in relation to the network or service concerned, non-discriminatory, proportionate and transparent.

2. Specific obligations which may be imposed on providers of electronic communications networks and services under Articles 5(1), 5(2), 6 and 8 of Directive 2002/19/EC (Access Directive) and Articles 16, 17, 18 and 19 of Directive 2002/22/EC (Universal Service Directive) or on those designated to provide universal service under the said Directive shall be legally separate from the rights and obligations under the general authorisation. In order to achieve transparency for undertakings, the criteria and procedures for imposing such specific obligations on individual undertakings shall be referred to in the general authorisation.

3. The general authorisation shall only contain conditions which are specific for that sector and are set out in Part A of the Annex and shall not duplicate conditions which are applicable to undertakings by virtue of other national legislation.

4. Member States shall not duplicate the conditions of the general authorisation where they grant the right of use for radio frequencies or numbers.

Article 7
Procedure for limiting the number of rights of use to be granted for radio frequencies

1. Where a Member State is considering whether to limit the number of rights of use to be granted for radio frequencies, it shall inter alia:

   (a) give due weight to the need to maximise benefits for users and to facilitate the development of competition;

   (b) give all interested parties, including users and consumers, the opportunity to express their views on any limitation in accordance with Article 6 of Directive 2002/21/EC (Framework Directive);

   (c) publish any decision to limit the granting of rights of use, stating the reasons therefor;

   (d) after having determined the procedure, invite applications for rights of use; and

   (e) review the limitation at reasonable intervals or at the reasonable request of affected undertakings.

2. Where a Member State concludes that further rights of use for radio frequencies can be granted, it shall publish that conclusion and invite applications for such rights.

3. Where the granting of rights of use for radio frequencies needs to be limited, Member States shall grant such rights on the basis of selection criteria which must be objective, transparent, non-discriminatory and proportionate. Any such selection criteria must give due weight to the achievement of the objectives of Article 8 of Directive 2002/21/EC (Framework Directive).

4. Where competitive or comparative selection procedures are to be used, Member States may extend the maximum period of six weeks referred to in Article 5(3) for as long as necessary to ensure that such procedures are fair, reasonable, open and transparent to all interested parties, but by no longer than eight months.

   These time limits shall be without prejudice to any applicable international agreements relating to the use of radio frequencies and satellite coordination.

5. This Article is without prejudice to the transfer of rights of use for radio frequencies in accordance with Article 9 of Directive 2002/21/EC (Framework Directive).

Article 8
Harmonised assignment of radio frequencies

Where the usage of radio frequencies has been harmonised, access conditions and procedures have been agreed, and undertakings to which the radio frequencies shall be assigned have been selected in accordance with international agreements and Community rules, Member States shall grant the right of use for such radio frequencies in accordance therewith. Provided that all national conditions attached to the right to use the radio frequencies concerned have been satisfied in the case of a common selection procedure, Member States shall not

impose any further conditions, additional criteria or procedures which would restrict, alter or delay the correct implementation of the common assignment of such radio frequencies.

Article 9
Declarations to facilitate the exercise of rights to install facilities and rights of interconnection

At the request of an undertaking, national regulatory authorities shall, within one week, issue standardised declarations, confirming, where applicable, that the undertaking has submitted a notification under Article 3(2) and detailing under what circumstances any undertaking providing electronic communications networks or services under the general authorisation has the right to apply for rights to install facilities, negotiate interconnection, and/or obtain access or interconnection in order to facilitate the exercise of those rights for instance at other levels of government or in relation to other undertakings. Where appropriate such declarations may also be issued as an automatic reply following the notification referred to in Article 3(2).

Article 10
Compliance with the conditions of the general authorisation or of rights of use and with specific obligations

1. National regulatory authorities may require undertakings providing electronic communications networks or services covered by the general authorisation or enjoying rights of use for radio frequencies or numbers to provide information necessary to verify compliance with the conditions of the general authorisation or of rights of use or with the specific obligations referred to in Article 6(2), in accordance with Article 11.

2. Where a national regulatory authority finds that an undertaking does not comply with one or more of the conditions of the general authorisation, or of rights of use or with the specific obligations referred to in Article 6(2), it shall notify the undertaking of those findings and give the undertaking a reasonable opportunity to state its views or remedy any breaches within:

   - one month after notification, or
   - a shorter period agreed by the undertaking or stipulated by the national regulatory authority in case of repeated breaches, or
   - a longer period decided by the national regulatory authority.

3. If the undertaking concerned does not remedy the breaches within the period as referred to in paragraph 2, the relevant authority shall take appropriate and proportionate measures aimed at ensuring compliance. In this regard, Member States may empower the relevant authorities to impose financial penalties where appropriate. The measures and the reasons on which they are based shall be communicated to the undertaking concerned within one week of their adoption and shall stipulate a reasonable period for the undertaking to comply with the measure.

4. Notwithstanding the provisions of paragraphs 2 and 3, Member States may empower the relevant authority to impose financial penalties where appropriate on undertakings for failure to provide information in accordance with obligations imposed under Article 11(1)(a) or (b) of this Directive or Article 9 of Directive 2002/19/EC (Access Directive) within a reasonable period stipulated by the national regulatory authority.

5. In cases of serious and repeated breaches of the conditions of the general authorisation, the rights of use or specific obligations referred to in Article 6(2), where measures aimed at ensuring compliance as referred to in paragraph 3 of this Article have failed, national regulatory authorities may prevent an undertaking from continuing to provide electronic communications networks or services or suspend or withdraw rights of use.

6. Irrespective of the provisions of paragraphs 2, 3 and 5, where the relevant authority has evidence of a breach of the conditions of the general authorisation, rights of use or specific obligations referred to in Article 6(2) that represents an immediate and serious threat to public safety, public security or public health or will create serious economic or operational problems for other providers or users of electronic communications networks or services, it may take urgent interim measures to remedy the situation in advance of reaching a final decision. The undertaking concerned shall thereafter be given a reasonable opportunity to state its view and propose any remedies. Where appropriate, the relevant authority may confirm the interim measures.

7. Undertakings shall have the right to appeal against measures taken under this Article in accordance with the procedure referred to in Article 4 of Directive 2002/21/EC (Framework

Directive).

Article 11
Information required under the general authorisation, for rights of use and for the specific obligations

1. Without prejudice to information and reporting obligations under national legislation other than the general authorisation, national regulatory authorities may only require undertakings to provide information under the general authorisation, for rights of use or the specific obligations referred to in Article 6(2) that is proportionate and objectively justified for:

   (a) systematic or case-by-case verification of compliance with conditions 1 and 2 of Part A, condition 6 of Part B and condition 7 of Part C of the Annex and of compliance with obligations as referred to in Article 6(2);

   (b) case-by-case verification of compliance with conditions as set out in the Annex where a complaint has been received or where the national regulatory authority has other reasons to believe that a condition is not complied with or in case of an investigation by the national regulatory authority on its own initiative;

   (c) procedures for and assessment of requests for granting rights of use;

   (d) publication of comparative overviews of quality and price of services for the benefit of consumers;

   (e) clearly defined statistical purposes;

   (f) market analysis for the purposes of Directive 2002/19/EC (Access Directive) or Directive 2002/22/EC (Universal Service Directive).

   The information referred to in points (a), (b), (d), (e) and (f) of the first subparagraph may not be required prior to or as a condition for market access.

2. Where national regulatory authorities require undertakings to provide information as referred to in paragraph 1, they shall inform them of the specific purpose for which this information is to be used.

Article 12
Administrative charges

1. Any administrative charges imposed on undertakings providing a service or a network under the general authorisation or to whom a right of use has been granted shall:

   (a) in total, cover only the administrative costs which will be incurred in the management, control and enforcement of the general authorisation scheme and of rights of use and of specific obligations as referred to in Article 6(2), which may include costs for international cooperation, harmonisation and standardisation, market analysis, monitoring compliance and other market control, as well as regulatory work involving preparation and enforcement of secondary legislation and administrative decisions, such as decisions on access and interconnection; and

   (b) be imposed upon the individual undertakings in an objective, transparent and proportionate manner which minimises additional administrative costs and attendant charges.

2. Where national regulatory authorities impose administrative charges, they shall publish a yearly overview of their administrative costs and of the total sum of the charges collected. In the light of the difference between the total sum of the charges and the administrative costs, appropriate adjustments shall be made.

Article 13
Fees for rights of use and rights to install facilities

Member States may allow the relevant authority to impose fees for the rights of use for radio frequencies or numbers or rights to install facilities on, over or under public or private property which reflect the need to ensure the optimal use of these resources. Member States shall ensure that such fees shall be objectively justified, transparent, non-discriminatory and proportionate in relation to their intended purpose and shall take into account the objectives in Article 8 of Directive 2002/21/EC (Framework Directive).

Article 14
Amendment of rights and obligations

1. Member States shall ensure that the rights, conditions and procedures concerning general authorisations and rights of use or rights to install facilities may only be amended in objectively justified cases and in a proportionate manner. Notice shall be given in an appropriate manner of the intention to make such amendments and interested parties, including users and consum-

ers, shall be allowed a sufficient period of time to express their views on the proposed amendments, which shall be no less than four weeks except in exceptional circumstances.

2. Member States shall not restrict or withdraw rights to install facilities before expiry of the period for which they were granted except where justified and where applicable in conformity with relevant national provisions regarding compensation for withdrawal of rights.

Article 15
Publication of information

1. Member States shall ensure that all relevant information on rights, conditions, procedures, charges, fees and decisions concerning general authorisations and rights of use is published and kept up to date in an appropriate manner so as to provide easy access to that information for all interested parties.

2. Where information as referred to in paragraph 1 is held at different levels of government, in particular information regarding procedures and conditions on rights to install facilities, the national regulatory authority shall make all reasonable efforts, bearing in mind the costs involved, to create a user-friendly overview of all such information, including information on the relevant levels of government and the responsible authorities, in order to facilitate applications for rights to install facilities.

Article 16
Review procedures

The Commission shall periodically review the functioning of the national authorisation systems and the development of cross-border service provision within the Community and report to the European Parliament and to the Council on the first occasion not later than three years after the date of application of this Directive referred to in Article 18(1), second subparagraph. For this purpose, the Commission may request from the Member States information, which shall be supplied without undue delay.

Article 17
Existing authorisations

1. Member States shall bring authorisations already in existence on the date of entry into force of this Directive into line with the provisions of this Directive by at the latest the date of application referred to in Article 18(1), second subparagraph.

2. Where application of paragraph 1 results in a reduction of the rights or an extension of the obligations under authorisations already in existence, Member States may extend the validity of those rights and obligations until at the latest nine months after the date of application referred to in Article 18(1), second subparagraph, provided that the rights of other undertakings under Community law are not affected thereby. Member States shall notify such extensions to the Commission and state the reasons therefor.

3. Where the Member State concerned can prove that the abolition of an authorisation condition regarding access to electronic communications networks, which was in force before the date of entry into force of this Directive, creates excessive difficulties for undertakings that have benefited from mandated access to another network, and where it is not possible for these undertakings to negotiate new agreements on reasonable commercial terms before the date of application referred to in Article 18(1), second subparagraph, Member States may request a temporary prolongation of the relevant condition(s). Such requests shall be submitted by the date of application referred to in Article 18(1), second subparagraph, at the latest, and shall specify the condition(s) and period for which the temporary prolongation is requested.

   The Member State shall inform the Commission of the reasons for requesting a prolongation. The Commission shall consider such a request, taking into account the particular situation in that Member State and of the undertaking(s) concerned, and the need to ensure a coherent regulatory environment at a Community level. It shall take a decision on whether to grant or reject the request, and where it decides to grant the request, on the scope and duration of the prolongation to be granted. The Commission shall communicate its decision to the Member State concerned within six months after receipt of the application for a prolongation. Such decisions shall be published in the Official Journal of the European Communities.

Article 18
Transposition

1. Member States shall adopt and publish the laws, regulations and administrative provisions necessary to comply with this Directive by 24 July 2003 at the latest. They shall forthwith inform the Commission thereof.

They shall apply those measures from 25 July 2003.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive and of any subsequent amendments to those provisions.

Article 19
Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 20
Addressees

This Directive is addressed to the Member States.

Done at Brussels, 7 March 2002.
For the European Parliament
The President P. Cox
For the Council
The President J. C. Aparicio

[1] OJ C 365 E, 19.12.2000, p. 230 and OJ C 270 E, 25.9.2001, p. 182.

[2] OJ C 123, 25.4.2001, p. 55.

[3] Opinion of the European Parliament of 1 March 2001 (OJ C 277, 1.10.2001, p. 116), Council Common Position of 17 September 2001 (OJ C 337, 30.11.2001, p. 18) and Decision of the European Parliament of 12 December 2001(not yet published in the Official Journal). Council Decision of 14 February 2002.

[4] OJ L 91, 7.4.1999, p. 10.

[5] OJ L 320, 28.11.1998, p. 54.

[6] See page 7 of this Official Journal.

[7] See page 33 of this Official Journal.

[8] See page 51 of this Official Journal.

ANNEX

The conditions listed in this Annex provide the maximum list of conditions which may be attached to general authorisations (Part A), rights to use radio frequencies (Part B) and rights to use numbers (Part C) as referred to in Article 6(1) and Article 11(1)(a).

A. Conditions which may be attached to a general authorisation

1. Financial contributions to the funding of universal service in conformity with Directive 2002/22/EC (Universal Service Directive).

2. Administrative charges in accordance with Article 12 of this Directive.

3. Interoperability of services and interconnection of networks in conformity with Directive 2002/19/EC (Access Directive).

4. Accessibility of numbers from the national numbering plan to end-users including conditions in conformity with Directive 2002/22/EC (Universal Service Directive).

5. Environmental and town and country planning requirements, as well as requirements and conditions linked to the granting of access to or use of public or private land and conditions linked to co-location and facility sharing in conformity with Directive 2002/22/EC (Framework Directive) and including, where applicable, any financial or technical guarantees necessary to ensure the proper execution of infrastructure works.

6. "Must carry" obligations in conformity with Directive 2002/22/EC (Universal Service Directive).

7. Personal data and privacy protection specific to the electronic communications sector in conformity with Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(1).

8. Consumer protection rules specific to the electronic communications sector including conditions in conformity with Directive 2002/22/EC (Universal Service Directive).

9. Restrictions in relation to the transmission of illegal content, in accordance with Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market(2) and restrictions in relation to the transmission of harmful content in accordance with Article 2a(2) of Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, regulation

or administrative action in Member States concerning the pursuit of television broadcasting activities(3).

10. Information to be provided under a notification procedure in accordance with Article 3(3) of this Directive and for other purposes as included in Article 11 of this Directive.

11. Enabling of legal interception by competent national authorities in conformity with Directive 97/66/EC and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data(4).

12. Terms of use during major disasters to ensure communications between emergency services and authorities and broadcasts to the general public.

13. Measures regarding the limitation of exposure of the general public to electromagnetic fields caused by electronic communications networks in accordance with Community law.

14. Access obligations other than those provided for in Article 6(2) of this Directive applying to undertakings providing electronic communications networks or services, in conformity with Directive 2002/19/EC (Access Directive).

15. Maintenance of the integrity of public communications networks in accordance with Directive 2002/19/EC (Access Directive) and Directive 2002/22/EC (Universal Service Directive) including by conditions to prevent electromagnetic interference between electronic communications networks and/or services in accordance with Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of the Member States relating to electromagnetic compatibility(5).

16. Security of public networks against unauthorised access according to Directive 97/66/EC.

17. Conditions for the use of radio frequencies, in conformity with Article 7(2) of Directive 1999/5/EC, where such use is not made subject to the granting of individual rights of use in accordance with Article 5(1) of this Directive.

18. Measures designed to ensure compliance with the standards and/or specifications referred to in Article 17 of Directive 2002/21/EC (Framework Directive).

B. Conditions which may be attached to rights of use for radio frequencies

1. Designation of service or type of network or technology for which the rights of use for the frequency has been granted, including, where applicable, the exclusive use of a frequency for the transmission of specific content or specific audiovisual services.

2. Effective and efficient use of frequencies in conformity with Directive 2002/21/EC (Framework Directive), including, where appropriate, coverage requirements.

3. Technical and operational conditions necessary for the avoidance of harmful interference and for the limitation of exposure of the general public to electromagnetic fields, where such conditions are different from those included in the general authorisation.

4. Maximum duration in conformity with Article 5 of this Directive, subject to any changes in the national frequency plan.

5. Transfer of rights at the initiative of the right holder and conditions for such transfer in conformity with Directive 2002/21/EC (Framework Directive).

6. Usage fees in accordance with Article 13 of this Directive.

7. Any commitments which the undertaking obtaining the usage right has made in the course of a competitive or comparative selection procedure.

8. Obligations under relevant international agreements relating to the use of frequencies.

C. Conditions which may be attached to rights of use for numbers

1. Designation of service for which the number shall be used, including any requirements linked to the provision of that service.

2. Effective and efficient use of numbers in conformity with Directive 2002/21/EC (Framework Directive).

3. Number portability requirements in conformity with Directive 2002/22/EC (Universal Service Directive).

4. Obligation to provide public directory subscriber information for the purposes of Articles 5 and 25 of Directive 2002/22/EC (Universal Service Directive).

5. Maximum duration in conformity with Article 5 of this Directive, subject to any changes in the national numbering plan.
6. Transfer of rights at the initiative of the right holder and conditions for such transfer in conformity with Directive 2002/21/EC (Framework Directive).
7. Usage fees in accordance with Article 13 of this Directive.
8. Any commitments which the undertaking obtaining the usage right has made in the course of a competitive or comparative selection procedure.
9. Obligations under relevant international agreements relating to the use of numbers.

[1] OJ L 24, 30.1.1998, p. 1.

[2] OJ L 178, 17.7.2000, p. 1.

[3] OJ L 298, 17.10.1989, p. 23. Directive as amended by Directive 97/36/EC of the European Parliament and of the Council (OJ L 202, 30.7.1997, p. 60).

[4] OJ L 281, 23.11.1995, p. 31.

[5] OJ L 139, 23.5.1989, p. 19. Directive as last amended by Directive 93/68/EEC (OJ L 220, 30.8.1993, p. 1).

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission(1),

Having regard to the opinion of the Economic and Social Committee(2),

Acting in accordance with the procedure laid down in Article 251 of the Treaty(3),

Whereas:

(1) The current regulatory framework for telecommunications has been successful in creating the conditions for effective competition in the telecommunications sector during the transition from monopoly to full competition.

(2) On 10 November 1999, the Commission presented a communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions entitled "Towards a new framework for electronic communications infrastructure and associated services - the 1999 communications review". In that communication, the Commission reviewed the existing regulatory framework for telecommunications, in accordance with its obligation under Article 8 of Council Directive 90/387/EEC of 28 June 1990 on the establishment of the internal market for telecommunications services through the implementation of open network provision(4). It also presented a series of policy proposals for a new regulatory framework for electronic communications infrastructure and associated services for public consultation.

(3) On 26 April 2000 the Commission presented a communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on the results of the public consultation on the 1999 communications review and orientations for the new regulatory framework. The communication summarised the public consultation and set out certain key orientations for the preparation of a new framework for electronic communications infrastructure and associated services.

(4) The Lisbon European Council of 23 and 24 March 2000 highlighted the potential for growth, competitiveness and job creation of the shift to a digital, knowledge-based economy. In particular, it emphasised the importance for Europe's businesses and citizens of access to an inexpensive, world-class communications infrastructure and a wide range of services.

(5) The convergence of the telecommunications, media and information technology sectors means all transmission networks and services should be covered by a single regulatory framework. That regulatory framework consists of this Directive and four specific Directives: Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive)(5), Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive)(6), Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)(7), Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(8), (hereinafter referred to as "the Specific Directives"). It is necessary to separate the regulation of transmission from the regulation of content. This framework does not therefore cover the content of services delivered over electronic communications networks using electronic communications services, such as broadcasting content, financial services and certain information society services, and is therefore without prejudice to measures taken at Community or national level in respect of such services, in compliance with Community law, in order to promote cultural and linguistic diversity and to ensure the defence of media pluralism. The content of television programmes is covered by Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities(9). The separation between the regulation of transmission and the regulation of content does not prejudice the taking into account of the links existing between them, in particular in order to guarantee media pluralism, cultural diversity and consumer protection.

(6) Audiovisual policy and content regulation are undertaken in pursuit of general interest objectives, such as freedom of expression, media pluralism, impartiality, cultural and linguistic diversity, social inclusion, consumer protection and the protection of minors. The Commission communication "Principles and guidelines for the Community's audio-visual policy in the digital age", and the Council conclusions of 6 June 2000 welcoming this communication, set out the key actions to be taken by the Community to implement its audio-visual policy.

(7) The provisions of this Directive and the Specific Directives are without prejudice to the possibility for each Member State to take the necessary measures to ensure the protection of its essential security interests, to safeguard public policy and public security, and to permit the investigation, detection and prosecution of criminal offences, including the establishment by national regulatory authorities of specific and proportional obligations applicable to providers of electronic communications services.

(8) This Directive does not cover equipment within the scope of Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity(10), but does cover consumer equipment used for digital television. It is important for regulators to encourage network operators and terminal equipment manufacturers to cooperate in order to facilitate access by disabled users to electronic communications services.

(9) Information society services are covered by Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce)(11).

(10) The definition of "information society service" in

Article 1 of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules of information society services(12) spans a wide range of economic activities which take place on-line. Most of these activities are not covered by the scope of this Directive because they do not consist wholly or mainly in the conveyance of signals on electronic communications networks. Voice telephony and electronic mail conveyance services are covered by this Directive. The same undertaking, for example an Internet service provider, can offer both an electronic communications service, such as access to the Internet, and services not covered under this Directive, such as the provision of web-based content.

(11) In accordance with the principle of the separation of regulatory and operational functions, Member States should guarantee the independence of the national regulatory authority or authorities with a view to ensuring the impartiality of their decisions. This requirement of independence is without prejudice to the institutional autonomy and constitutional obligations of the Member States or to the principle of neutrality with regard to the rules in Member States governing the system of property ownership laid down in Article 295 of the Treaty. National regulatory authorities should be in possession of all the necessary resources, in terms of staffing, expertise, and financial means, for the performance of their tasks.

(12) Any party who is the subject of a decision by a national regulatory authority should have the right to appeal to a body that is independent of the parties involved. This body may be a court. Furthermore, any undertaking which considers that its applications for the granting of rights to install facilities have not been dealt with in accordance with the principles set out in this Directive should be entitled to appeal against such decisions. This appeal procedure is without prejudice to the division of competences within national judicial systems and to the rights of legal entities or natural persons under national law.

(13) National regulatory authorities need to gather information from market players in order to carry out their tasks effectively. Such information may also need to be gathered on behalf of the Commission, to allow it to fulfil its obligations under Community law. Requests for information should be proportionate and not impose an undue burden on undertakings. Information gathered by national regulatory authorities should be publicly available, except in so far as it is confidential in accordance with national rules on public access to information and subject to Community and national law on business confidentiality.

(14) Information that is considered confidential by a national regulatory authority, in accordance with Community and national rules on business confidentiality, may only be exchanged with the Commission and other national regulatory authorities where such exchange is strictly necessary for the application of the provisions of this Directive or the Specific Directives. The information exchanged should be limited to that which is relevant and proportionate to the purpose of such an exchange.

(15) It is important that national regulatory authorities consult all interested parties on proposed decisions and take account of their comments before adopting a final decision. In order to ensure that decisions at national level do not have an adverse effect on the single market or other Treaty objectives, national regulatory authorities should also notify certain draft decisions to the Commission and other national regulatory authorities to give them the opportunity to comment. It is appropriate for national regulatory authorities to consult interested parties on all draft measures which have an effect on trade between Member States. The cases where the procedures referred to in Articles 6 and 7 apply are defined in this Directive and in the Specific Directives. The Commission should be able, after consulting the Communications Committee, to require a national regulatory authority to withdraw a draft measure where it concerns definition of relevant markets or the designation or not of undertakings with significant market power, and where such decisions would create a barrier to the single market or would be incompatible with Community law and in particular the policy objectives that national regulatory authorities should follow. This procedure is without prejudice to the notification procedure provided for in Directive 98/34/EC and the Commission's prerogatives under the Treaty in respect of infringements of Community law.

(16) National regulatory authorities should have a harmonised set of objectives and principles to underpin, and should, where necessary, coordinate their actions with the regulatory authorities of other Member States in carrying out their tasks under this regulatory framework.

(17) The activities of national regulatory authorities established under this Directive and the Specific Directives contribute to the fulfilment of broader policies in the areas of culture, employment, the environment, social cohesion and town and country planning.

(18) The requirement for Member States to ensure that national regulatory authorities take the utmost account of the desirability of making regulation technologically neutral, that is to say that it neither imposes nor discriminates in favour of the use of a particular type of technology, does not preclude the taking of proportionate steps to promote certain specific services where this is justified, for example digital television as a means for increasing spectrum efficiency.

(19) Radio frequencies are an essential input for radio-based electronic communications services and, in so far as they relate to such services, should therefore be allocated and assigned by national regulatory authorities according to a set of harmonised objectives and principles governing their action as well as to objective, transparent and non-discriminatory criteria, taking into account the democratic, social, linguistic and cultural interests related to the use of frequency. It is important that the allocation and assignment of radio frequencies is managed as efficiently as possible. Transfer of radio frequencies can be an effective means of increasing efficient use of spectrum, as long as there are sufficient safeguards in place to protect the public interest, in particular the need to ensure transparency and regulatory supervision of such transfers. Decision No 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision)(13) establishes a framework for harmonisation of radio frequencies, and action taken under this Directive should seek to facilitate the work under that Decision.

(20) Access to numbering resources on the basis of transparent, objective and non-discriminatory criteria is essential for undertakings to compete in the electronic communications sector. All elements of national numbering plans should be managed by national regulatory authorities, including point codes used in network addressing. Where there is a need for harmonisation of numbering resources in the Community to support the development of pan-European services, the Commission may take technical implementing measures using its executive powers. Where this is appropriate to ensure full global interoperability of services, Member States should coordinate their national positions in accordance with the Treaty in international organisations and fora where numbering decisions are taken. The provisions of this Directive do not establish any new areas of responsibility for the national regulatory authorities in the field of Internet naming and addressing.

(21) Member States may use, inter alia, competitive or comparative selection procedures for the assignment of radio frequencies as well as numbers with exceptional economic value. In administering such schemes, national regulatory authorities should take into account the provisions of Article 8.

(22) It should be ensured that procedures exist for the granting of rights to install facilities that are timely, non-discriminatory and transparent, in order to guarantee the conditions for fair and effective competition. This Directive is without prejudice to national provisions governing the expropriation or use of property, the normal exercise of property rights, the normal use of the public domain, or to the principle of neutrality with regard to the rules in Member States governing the system of property ownership.

(23) Facility sharing can be of benefit for town planning, public health or environmental reasons, and should be encouraged by national regulatory authorities on the basis of voluntary agreements. In cases where undertakings are deprived of access to viable alternatives, compulsory facility or property sharing may be appropriate. It covers inter alia: physical co-location and duct, building, mast, antenna or antenna system sharing. Compulsory facility or property sharing should be imposed on undertakings only after full public consultation.

(24) Where mobile operators are required to share towers or masts for environmental reasons, such mandated sharing may lead to a reduction in the maximum transmitted power levels allowed for each operator for reasons of public health, and this in turn may require operators to install more transmission sites to ensure national coverage.

(25) There is a need for ex ante obligations in certain circumstances in order to ensure the development of a competitive market. The definition of significant market power in the Directive 97/33/EC of the European Parliament and of the Council of 30 June 1997 on interconnection in telecommunications with regard to ensuring

universal service and interoperability through application of the principles of open network provision (ONP)(14) has proved effective in the initial stages of market opening as the threshold for ex ante obligations, but now needs to be adapted to suit more complex and dynamic markets. For this reason, the definition used in this Directive is equivalent to the concept of dominance as defined in the case law of the Court of Justice and the Court of First Instance of the European Communities.

(26) Two or more undertakings can be found to enjoy a joint dominant position not only where there exist structural or other links between them but also where the structure of the relevant market is conducive to coordinated effects, that is, it encourages parallel or aligned anti-competitive behaviour on the market.

(27) It is essential that ex ante regulatory obligations should only be imposed where there is not effective competition, i.e. in markets where there are one or more undertakings with significant market power, and where national and Community competition law remedies are not sufficient to address the problem. It is necessary therefore for the Commission to draw up guidelines at Community level in accordance with the principles of competition law for national regulatory authorities to follow in assessing whether competition is effective in a given market and in assessing significant market power. National regulatory authorities should analyse whether a given product or service market is effectively competitive in a given geographical area, which could be the whole or a part of the territory of the Member State concerned or neighbouring parts of territories of Member States considered together. An analysis of effective competition should include an analysis as to whether the market is prospectively competitive, and thus whether any lack of effective competition is durable. Those guidelines will also address the issue of newly emerging markets, where de facto the market leader is likely to have a substantial market share but should not be subjected to inappropriate obligations. The Commission should review the guidelines regularly to ensure that they remain appropriate in a rapidly developing market. National regulatory authorities will need to cooperate with each other where the relevant market is found to be transnational.

(28) In determining whether an undertaking has significant market power in a specific market, national regulatory authorities should act in accordance with Community law and take into the utmost account the Commission guidelines.

(29) The Community and the Member States have entered into commitments in relation to standards and the regulatory framework of telecommunications networks and services in the World Trade Organisation.

(30) Standardisation should remain primarily a market-driven process. However there may still be situations where it is appropriate to require compliance with specified standards at Community level to ensure interoperability in the single market. At national level, Member States are subject to the provisions of Directive 98/34/EC. Directive 95/47/EC of the European Parliament and of the Council of 24 October 1995 on the use of standards for the transmission of television signals(15) did not mandate any specific digital television transmission system or service requirement. Through the Digital Video Broadcasting Group, European market players have developed a family of television transmission systems that have been standardised by the European Telecommunications Standards Institute (ETSI) and have become International Telecommunication Union recommendations. Any decision to make the implementation of such standards mandatory should follow a full public consultation. Standardisation procedures under this Directive are without prejudice to the provisions of Directive 1999/5/EC, Council Directive 73/23/EEC of 19 February 1973 on the harmonisation of the laws of Member States relating to electrical equipment designed for use within certain voltage limits(16) and Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of the Member States relating to electromagnetic compatibility(17).

(31) Interoperability of digital interactive television services and enhanced digital television equipment, at the level of the consumer, should be encouraged in order to ensure the free flow of information, media pluralism and cultural diversity. It is desirable for consumers to have the capability of receiving, regardless of the transmission mode, all digital interactive television services, having regard to technological neutrality, future technological progress, the need to promote the take-up of digital television, and the state of competition in the markets for digital television services. Digital interactive television platform operators should strive to implement an open application program interface (API) which conforms to standards or specifications adopted by a European stand-

ards organisation. Migration from existing APIs to new open APIs should be encouraged and organised, for example by Memoranda of Understanding between all relevant market players. Open APIs facilitate interoperability, i.e. the portability of interactive content between delivery mechanisms, and full functionality of this content on enhanced digital television equipment. However, the need not to hinder the functioning of the receiving equipment and to protect it from malicious attacks, for example from viruses, should be taken into account.

(32) In the event of a dispute between undertakings in the same Member State in an area covered by this Directive or the Specific Directives, for example relating to obligations for access and interconnection or to the means of transferring subscriber lists, an aggrieved party that has negotiated in good faith but failed to reach agreement should be able to call on the national regulatory authority to resolve the dispute. National regulatory authorities should be able to impose a solution on the parties. The intervention of a national regulatory authority in the resolution of a dispute between undertakings providing electronic communications networks or services in a Member State should seek to ensure compliance with the obligations arising under this Directive or the Specific Directives.

(33) In addition to the rights of recourse granted under national or Community law, there is a need for a simple procedure to be initiated at the request of either party in a dispute, to resolve cross-border disputes which lie outside the competence of a single national regulatory authority.

(34) A single Committee should replace the "ONP Committee" instituted by Article 9 of Directive 90/387/EEC and the Licensing Committee instituted by Article 14 of Directive 97/13/EC of the European Parliament and of the Council of 10 April 1997 on a common framework for general authorisations and individual licences in the field of telecommunications services(18).

(35) National regulatory authorities and national competition authorities should provide each other with the information necessary to apply the provisions of this Directive and the Specific Directives, in order to allow them to cooperate fully together. In respect of the information exchanged, the receiving authority should ensure the same level of confidentiality as the originating authority.

(36) The Commission has indicated its intention to set up a European regulators group for electronic communications networks and services which would constitute a suitable mechanism for encouraging cooperation and coordination of national regulatory authorities, in order to promote the development of the internal market for electronic communications networks and services, and to seek to achieve consistent application, in all Member States, of the provisions set out in this Directive and the Specific Directives, in particular in areas where national law implementing Community law gives national regulatory authorities considerable discretionary powers in application of the relevant rules.

(37) National regulatory authorities should be required to cooperate with each other and with the Commission in a transparent manner to ensure consistent application, in all Member States, of the provisions of this Directive and the Specific Directives. This cooperation could take place, inter alia, in the Communications Committee or in a group comprising European regulators. Member States should decide which bodies are national regulatory authorities for the purposes of this Directive and the Specific Directives.

(38) Measures that could affect trade between Member States are measures that may have an influence, direct or indirect, actual or potential, on the pattern of trade between Member States in a manner which might create a barrier to the single market. They comprise measures that have a significant impact on operators or users in other Member States, which include, inter alia: measures which affect prices for users in other Member States; measures which affect the ability of an undertaking established in another Member State to provide an electronic communications service, and in particular measures which affect the ability to offer services on a transnational basis; and measures which affect market structure or access, leading to repercussions for undertakings in other Member States.

(39) The provisions of this Directive should be reviewed periodically, in particular with a view to determining the need for modification in the light of changing technological or market conditions.

(40) The measures necessary for the implementation of this Directive should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for

the exercise of implementing powers conferred on the Commission(19).

(41) Since the objectives of the proposed action, namely achieving a harmonised framework for the regulation of electronic communications services, electronic communications networks, associated facilities and associated services cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of the action, be better achieved at Community level, the Community may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary for those objectives.

(42) Certain directives and decisions in this field should be repealed.

(43) The Commission should monitor the transition from the existing framework to the new framework, and may in particular, at an appropriate time, bring forward a proposal to repeal Regulation (EC) No 2887/2000 of the European Parliament and of the Council of 18 December 2000 on unbundled access to the local loop(20),

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I
SCOPE, AIM AND DEFINITIONS

Article 1
Scope and aim

1. This Directive establishes a harmonised framework for the regulation of electronic communications services, electronic communications networks, associated facilities and associated services. It lays down tasks of national regulatory authorities and establishes a set of procedures to ensure the harmonised application of the regulatory framework throughout the Community.

2. This Directive as well as the Specific Directives are without prejudice to obligations imposed by national law in accordance with Community law or by Community law in respect of services provided using electronic communications networks and services.

3. This Directive as well as the Specific Directives are without prejudice to measures taken at Community or national level, in compliance with Community law, to pursue general interest objectives, in particular relating to content regulation and audio-visual policy.

4. This Directive and the Specific Directives are without prejudice to the provisions of Directive 1999/5/EC.

Article 2
Definitions

For the purposes of this Directive:

(a) "electronic communications network" means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

(b) "transnational markets" means markets identified in accordance with Article 15(4) covering the Community or a substantial part thereof;

(c) "electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks;

(d) "public communications network" means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services;

(e) "associated facilities" means those facilities associated with an electronic communications network and/or an electronic communications service which enable and/or support the provision of services via that network and/or service. It includes conditional access systems and electronic programme guides;

(f) "conditional access system" means any technical measure and/or arrangement whereby access to a protected radio or television broadcasting service in intelligible form is made conditional upon subscription or other form of prior individual authorisation;

(g) "national regulatory authority" means the body or bodies charged by a Member State with any of the regulatory tasks assigned in this Directive and the Specific Directives;

(h) "user" means a legal entity or natural person using or requesting a publicly available electronic communications service;

(i) "consumer" means any natural person who uses or requests a publicly available electronic communications service for purposes which are outside his or her trade, business or profession;

(j) "universal service" means the minimum set of services, defined in Directive 2002/22/EC (Universal Service Directive), of specified quality which is available to all users regardless of their geographical location and, in the light of specific national conditions, at an affordable price;

(k) "subscriber" means any natural person or legal entity who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such services;

(l) "Specific Directives" means Directive 2002/20/EC (Authorisation Directive), Directive 2002/19/EC (Access Directive), Directive 2002/22/EC (Universal Service Directive) and Directive 97/66/EC;

(m) "provision of an electronic communications network" means the establishment, operation, control or making available of such a network;

(n) "end-user" means a user not providing public communications networks or publicly available electronic communications services.

(o) "enhanced digital television equipment" means set-top boxes intended for connection to television sets or integrated digital television sets, able to receive digital interactive television services;

(p) "application program interface (API)" means the software interfaces between applications, made available by broadcasters or service providers, and the resources in the enhanced digital television equipment for digital television and radio services.

CHAPTER II
NATIONAL REGULATORY AUTHORITIES

Article 3
National regulatory authorities

1. Member States shall ensure that each of the tasks assigned to national regulatory authorities in this Directive and the Specific Directives is undertaken by a competent body.

2. Member States shall guarantee the independence of national regulatory authorities by ensuring that they are legally distinct from and functionally independent of all organisations providing electronic communications networks, equipment or services. Member States that retain ownership or control of undertakings providing electronic communications networks and/or services shall ensure effective structural separation of the regulatory function from activities associated with ownership or control.

3. Member States shall ensure that national regulatory authorities exercise their powers impartially and transparently.

4. Member States shall publish the tasks to be undertaken by national regulatory authorities in an easily accessible form, in particular where those tasks are assigned to more than one body. Member States shall ensure, where appropriate, consultation and cooperation between those authorities, and between those authorities and national authorities entrusted with the implementation of competition law and national authorities entrusted with the implementation of consumer law, on matters of common interest. Where more than one authority has competence to address such matters, Member States shall ensure that the respective tasks of each authority are published in an easily accessible form.

5. National regulatory authorities and national competition authorities shall provide each other with the information necessary for the application of the provisions of this Directive and the Specific Directives. In respect of the information exchanged, the receiving authority shall ensure the same level of confidentiality as the originating authority.

6. Member States shall notify to the Commission all national regulatory authorities assigned tasks under this Directive and the Specific Directives, and their respective responsibilities.

Article 4
Right of appeal

1. Member States shall ensure that effective mechanisms exist at national level under which any user or undertaking providing electronic communications networks and/or services who is affected by a decision of a national regulatory authority has the right of appeal against the decision to an appeal body that is independent of the parties involved. This body, which may be a court, shall have the appropriate expertise available to it to enable it to carry out its functions. Member States shall ensure that the merits of the case are duly taken into account and that there is an effective appeal mechanism. Pending the outcome of any such appeal, the decision of the national regulatory authority shall stand, unless the appeal body decides otherwise.

2. Where the appeal body referred to in paragraph 1 is not judicial in character, written reasons for its decision shall always be given. Furthermore, in such a case, its decision shall be subject to review by a court or tribunal within the meaning of Article 234 of the Treaty.

Article 5
Provision of information

1. Member States shall ensure that undertakings providing electronic communications networks and services provide all the information, including financial information, necessary for national regulatory authorities to ensure conformity with the provisions of, or decisions made in accordance with, this Directive and the Specific Directives. These undertakings shall provide such information promptly on request and to the timescales and level of detail required by the national regulatory authority. The information requested by the national regulatory authority shall be proportionate to the performance of that task. The national regulatory authority shall give the reasons justifying its request for information.

2. Member States shall ensure that national regulatory authorities provide the Commission, after a reasoned request, with the information necessary for it to carry out its tasks under the Treaty. The information requested by the Commission shall be proportionate to the performance of those tasks. Where the information provided refers to information previously provided by undertakings at the request of the national regulatory authority, such undertakings shall be informed thereof. To the extent necessary, and unless the authority that provides the information has made an explicit and reasoned request to the contrary, the Commission shall make the information provided available to another such authority in another Member State.

   Subject to the requirements of paragraph 3, Member States shall ensure that the information submitted to one national regulatory authority can be made available to another such authority in the same or different Member State, after a substantiated request, where necessary to allow either authority to fulfil its responsibilities under Community law.

3. Where information is considered confidential by a national regulatory authority in accordance with Community and national rules on business confidentiality, the Commission and the national regulatory authorities concerned shall ensure such confidentiality.

4. Member States shall ensure that, acting in accordance with national rules on public access to information and subject to Community and national rules on business confidentiality, national regulatory authorities publish such information as would contribute to an open and competitive market.

5. National regulatory authorities shall publish the terms of public access to information as referred to in paragraph 4, including procedures for obtaining such access.

Article 6
Consultation and transparency mechanism

Except in cases falling within Articles 7(6), 20 or 21 Member States shall ensure that where national regulatory authorities intend to take measures in accordance with this Directive or the Specific Directives which have a significant impact on the relevant market, they give interested parties the opportunity to comment on the draft measure within a reasonable period. National regulatory authorities shall publish their national consultation procedures. Member States shall ensure the establishment of a single information point through which all current consultations can be accessed. The results of the consultation procedure shall be made publicly available by the national regulatory authority, except in the case of confidential information in accordance with Community and national law on business confidentiality.

Article 7
Consolidating the internal market for electronic communications

1. In carrying out their tasks under this Directive and the Specific Directives, national regulatory authorities shall take the utmost account of the objectives set out in Article 8, including in so far as they relate to the functioning of the internal market.

2. National regulatory authorities shall contribute to the development of the internal market by cooperating with each other and with the Commission in a transparent manner to ensure the consistent application, in all Member States, of the provisions of this Directive and the Specific Directives. To this end, they shall, in particular, seek to agree on the types of instruments and remedies best suited to address particular types of situations in the market place.

3. In addition to the consultation referred to in Article 6, where a national regulatory authority intends to take a measure which:

   (a) falls within the scope of Articles 15 or 16 of this Directive, Articles 5 or 8 of Directive 2002/19/EC (Access Directive) or Article 16 of Directive 2002/22/EC (Universal Service Directive), and

   (b) would affect trade between Member States,

   it shall at the same time make the draft measure accessible to the Commission and the national regulatory authorities in other Member States, together with the reasoning on which the measure is based, in accordance with Article 5(3), and inform the Commission and other national regulatory authorities thereof. National regulatory authorities and the Commission may make comments to the national regulatory authority concerned only within one month or within the period referred to in Article 6 if that period is longer. The one-month period may not be extended.

4. Where an intended measure covered by paragraph 3 aims at:

   (a) defining a relevant market which differs from those defined in the recommendation in accordance with Article 15(1), or

   (b) deciding whether or not to designate an undertaking as having, either individually or jointly with others, significant market power, under Article 16(3), (4) or (5),

   and would affect trade between Member States and the Commission has indicated to the national regulatory authority that it considers that the draft measure would create a barrier to the single market or if it has serious doubts as to its compatibility with Community law and in particular the objectives referred to in Article 8, then the draft measure shall not be adopted for a further two months. This period may not be extended. Within this period the Commission may, in accordance with the procedure referred to in Article 22(2), take a decision requiring the national regulatory authority concerned to withdraw the draft measure. This decision shall be accompanied by a detailed and objective analysis of why the Commission considers that the draft measure should not be adopted together with specific proposals for amending the draft measure.

5. The national regulatory authority concerned shall take the utmost account of comments of other national regulatory authorities and the Commission and may, except in cases covered by paragraph 4, adopt the resulting draft measure and, where it does so, shall communicate it to the Commission.

6. In exceptional circumstances, where a national regulatory authority considers that there is an urgent need to act, by way of derogation from the procedure set out in paragraphs 3 and 4, in order to safeguard competition and protect the interests of users, it may immediately adopt proportionate and provisional measures. It shall, without delay, communicate those measures, with full reasons, to the Commission and the other national regulatory authorities. A decision by the national regulatory authority to render such measures permanent or extend the time for which they are applicable shall be subject to the provisions of paragraphs 3 and 4.

CHAPTER III
TASKS OF NATIONAL REGULATORY AUTHORITIES

Article 8
Policy objectives and regulatory principles

1. Member States shall ensure that in carrying out the regulatory tasks specified in this Directive and the Specific Directives, the national regulatory authorities take all reasonable measures which are aimed at achieving the objectives set out in paragraphs 2, 3 and 4. Such measures

shall be proportionate to those objectives.

Member States shall ensure that in carrying out the regulatory tasks specified in this Directive and the Specific Directives, in particular those designed to ensure effective competition, national regulatory authorities take the utmost account of the desirability of making regulations technologically neutral.

National regulatory authorities may contribute within their competencies to ensuring the implementation of policies aimed at the promotion of cultural and linguistic diversity, as well as media pluralism.

2. The national regulatory authorities shall promote competition in the provision of electronic communications networks, electronic communications services and associated facilities and services by inter alia:

   (a) ensuring that users, including disabled users, derive maximum benefit in terms of choice, price, and quality;

   (b) ensuring that there is no distortion or restriction of competition in the electronic communications sector;

   (c) encouraging efficient investment in infrastructure, and promoting innovation; and

   (d) encouraging efficient use and ensuring the effective management of radio frequencies and numbering resources.

3. The national regulatory authorities shall contribute to the development of the internal market by inter alia:

   (a) removing remaining obstacles to the provision of electronic communications networks, associated facilities and services and electronic communications services at European level;

   (b) encouraging the establishment and development of trans-European networks and the interoperability of pan-European services, and end-to-end connectivity;

   (c) ensuring that, in similar circumstances, there is no discrimination in the treatment of undertakings providing electronic communications networks and services;

   (d) cooperating with each other and with the Commission in a transparent manner to ensure the development of consistent regulatory practice and the consistent application of this Directive and the Specific Directives.

4. The national regulatory authorities shall promote the interests of the citizens of the European Union by inter alia:

   (a) ensuring all citizens have access to a universal service specified in Directive 2002/22/EC (Universal Service Directive);

   (b) ensuring a high level of protection for consumers in their dealings with suppliers, in particular by ensuring the availability of simple and inexpensive dispute resolution procedures carried out by a body that is independent of the parties involved;

   (c) contributing to ensuring a high level of protection of personal data and privacy;

   (d) promoting the provision of clear information, in particular requiring transparency of tariffs and conditions for using publicly available electronic communications services;

   (e) addressing the needs of specific social groups, in particular disabled users; and

   (f) ensuring that the integrity and security of public communications networks are maintained.

Article 9
Management of radio frequencies for electronic communications services

1. Member States shall ensure the effective management of radio frequencies for electronic communication services in their territory in accordance with Article 8. They shall ensure that the allocation and assignment of such radio frequencies by national regulatory authorities are based on objective, transparent, non-discriminatory and proportionate criteria.

2. Member States shall promote the harmonisation of use of radio frequencies across the Community, consistent with the need to ensure effective and efficient use thereof and in accordance with the Decision No 676/2002/EC (Radio Spectrum Decision).

3. Member States may make provision for undertakings to transfer rights to use radio frequencies with other undertakings.

4. Member States shall ensure that an undertaking's intention to transfer rights to use radio frequencies is notified to the national regulatory authority responsible for spectrum assignment

and that any transfer takes place in accordance with procedures laid down by the national regulatory authority and is made public. National regulatory authorities shall ensure that competition is not distorted as a result of any such transaction. Where radio frequency use has been harmonised through the application of Decision No 676/2002/EC (Radio Spectrum Decision) or other Community measures, any such transfer shall not result in change of use of that radio frequency.

Article 10
Numbering, naming and addressing

1. Member States shall ensure that national regulatory authorities control the assignment of all national numbering resources and the management of the national numbering plans. Member States shall ensure that adequate numbers and numbering ranges are provided for all publicly available electronic communications services. National regulatory authorities shall establish objective, transparent and non-discriminatory assigning procedures for national numbering resources.

2. National regulatory authorities shall ensure that numbering plans and procedures are applied in a manner that gives equal treatment to all providers of publicly available electronic communications services. In particular, Member States shall ensure that an undertaking allocated a range of numbers does not discriminate against other providers of electronic communications services as regards the number sequences used to give access to their services.

3. Member States shall ensure that the national numbering plans, and all subsequent additions or amendments thereto, are published, subject only to limitations imposed on the grounds of national security.

4. Member States shall support the harmonisation of numbering resources within the Community where that is necessary to support the development of pan European services. The Commission may, in accordance with the procedure referred to in Article 22(3), take the appropriate technical implementing measures on this matter.

5. Where this is appropriate in order to ensure full global interoperability of services, Member States shall coordinate their positions in international organisations and forums in which decisions are taken on issues relating to the numbering, naming and addressing of electronic communications networks and services.

Article 11
Rights of way

1. Member States shall ensure that when a competent authority considers:

   - an application for the granting of rights to install facilities on, over or under public or private property to an undertaking authorised to provide public communications networks, or
   - an application for the granting of rights to install facilities on, over or under public property to an undertaking authorised to provide electronic communications networks other than to the public,

   the competent authority:

   - acts on the basis of transparent and publicly available procedures, applied without discrimination and without delay, and
   - follows the principles of transparency and non-discrimination in attaching conditions to any such rights.

   The abovementioned procedures can differ depending on whether the applicant is providing public communications networks or not.

2. Member States shall ensure that where public or local authorities retain ownership or control of undertakings operating electronic communications networks and/or services, there is effective structural separation of the function responsible for granting the rights referred to in paragraph 1 from activities associated with ownership or control.

3. Member States shall ensure that effective mechanisms exist to allow undertakings to appeal against decisions on the granting of rights to install facilities to a body that is independent of the parties involved.

Article 12
Co-location and facility sharing

1. Where an undertaking providing electronic communications networks has the right under national legislation to install facilities on, over or under public or private property, or may take advantage of a procedure for the expropriation or use of property, national regulatory authorities shall encourage the sharing of such facilities or property.

2. In particular where undertakings are deprived of access to viable alternatives because of the need to protect the environment, public health, public security or to meet town and country planning objectives, Member States may impose the sharing of facilities or property (including physical co-location) on an undertaking operating an electronic communications network or take measures to facilitate the coordination of public works only after an appropriate period of public consultation during which all interested parties must be given an opportunity to express their views. Such sharing or coordination arrangements may include rules for apportioning the costs of facility or property sharing.

Article 13
Accounting separation and financial reports

1. Member States shall require undertakings providing public communications networks or publicly available electronic communications services which have special or exclusive rights for the provision of services in other sectors in the same or another Member State to:

   (a) keep separate accounts for the activities associated with the provision of electronic communications networks or services, to the extent that would be required if these activities were carried out by legally independent companies, so as to identify all elements of cost and revenue, with the basis of their calculation and the detailed attribution methods used, related to their activities associated with the provision of electronic communications networks or services including an itemised breakdown of fixed asset and structural costs, or

   (b) have structural separation for the activities associated with the provision of electronic communications networks or services.

   Member States may choose not to apply the requirements referred to in the first subparagraph to undertakings the annual turnover of which in activities associated with electronic communications networks or services in the Member States is less than EUR 50 million.

2. Where undertakings providing public communications networks or publicly available electronic communications services are not subject to the requirements of company law and do not satisfy the small and medium-sized enterprise criteria of Community law accounting rules, their financial reports shall be drawn up and submitted to independent audit and published. The audit shall be carried out in accordance with the relevant Community and national rules.

   This requirement shall also apply to the separate accounts required under paragraph 1(a).

CHAPTER IV
GENERAL PROVISIONS

Article 14
Undertakings with significant market power

1. Where the Specific Directives require national regulatory authorities to determine whether operators have significant market power in accordance with the procedure referred to in Article 16, paragraphs 2 and 3 of this Article shall apply.

2. An undertaking shall be deemed to have significant market power if, either individually or jointly with others, it enjoys a position equivalent to dominance, that is to say a position of economic strength affording it the power to behave to an appreciable extent independently of competitors, customers and ultimately consumers.

   In particular, national regulatory authorities shall, when assessing whether two or more undertakings are in a joint dominant position in a market, act in accordance with Community law and take into the utmost account the guidelines on market analysis and the assessment of significant market power published by the Commission pursuant to Article 15. Criteria to be used in making such an assessment are set out in Annex II.

3. Where an undertaking has significant market power on a specific market, it may also be deemed to have significant market power on a closely related market, where the links between the two markets are such as to allow the market power held in one market to be leveraged into the other market, thereby strengthening the market power of the undertaking.

Article 15
Market definition procedure

1. After public consultation and consultation with national regulatory authorities the Commission shall adopt a recommendation on relevant product and service markets (hereinafter "the recommendation"). The recommendation

shall identify in accordance with Annex I hereto those product and service markets within the electronic communications sector, the characteristics of which may be such as to justify the imposition of regulatory obligations set out in the Specific Directives, without prejudice to markets that may be defined in specific cases under competition law. The Commission shall define markets in accordance with the principles of competition law.

The Commission shall regularly review the recommendation.

2. The Commission shall publish, at the latest on the date of entry into force of this Directive, guidelines for market analysis and the assessment of significant market power (hereinafter "the guidelines") which shall be in accordance with the principles of competition law.

3. National regulatory authorities shall, taking the utmost account of the recommendation and the guidelines, define relevant markets appropriate to national circumstances, in particular relevant geographic markets within their territory, in accordance with the principles of competition law. National regulatory authorities shall follow the procedures referred to in Articles 6 and 7 before defining the markets that differ from those defined in the recommendation.

4. After consultation with national regulatory authorities the Commission may, acting in accordance with the procedure referred to in Article 22(3), adopt a Decision identifying transnational markets.

Article 16
Market analysis procedure

1. As soon as possible after the adoption of the recommendation or any updating thereof, national regulatory authorities shall carry out an analysis of the relevant markets, taking the utmost account of the guidelines. Member States shall ensure that this analysis is carried out, where appropriate, in collaboration with the national competition authorities.

2. Where a national regulatory authority is required under Articles 16, 17, 18 or 19 of Directive 2002/22/EC (Universal Service Directive), or Articles 7 or 8 of Directive 2002/19/EC (Access Directive) to determine whether to impose, maintain, amend or withdraw obligations on undertakings, it shall determine on the basis of its market analysis referred to in paragraph 1 of this Article whether a relevant market is effectively competitive.

3. Where a national regulatory authority concludes that the market is effectively competitive, it shall not impose or maintain any of the specific regulatory obligations referred to in paragraph 2 of this Article. In cases where sector specific regulatory obligations already exist, it shall withdraw such obligations placed on undertakings in that relevant market. An appropriate period of notice shall be given to parties affected by such a withdrawal of obligations.

4. Where a national regulatory authority determines that a relevant market is not effectively competitive, it shall identify undertakings with significant market power on that market in accordance with Article 14 and the national regulatory authority shall on such undertakings impose appropriate specific regulatory obligations referred to in paragraph 2 of this Article or maintain or amend such obligations where they already exist.

5. In the case of transnational markets identified in the Decision referred to in Article 15(4), the national regulatory authorities concerned shall jointly conduct the market analysis taking the utmost account of the guidelines and decide on any imposition, maintenance, amendment or withdrawal of regulatory obligations referred to in paragraph 2 of this Article in a concerted fashion.

6. Measures taken according to the provisions of paragraphs 3, 4 and 5 of this Article shall be subject to the procedures referred to in Articles 6 and 7.

Article 17
Standardisation

1. The Commission, acting in accordance with the procedure referred to in Article 22(2), shall draw up and publish in the Official Journal of the European Communities a list of standards and/or specifications to serve as a basis for encouraging the harmonised provision of electronic communications networks, electronic communications services and associated facilities and services. Where necessary, the Commission may, acting in accordance with the procedure referred to in Article 22(2) and following consultation of the Committee established by Directive 98/34/EC, request that standards be drawn up by the European standards organisations (European Committee for Standardisation (CEN), European Committee for Electrotechnical Standardisation

(CENELEC), and European Telecommunications Standards Institute (ETSI)).

2. Member States shall encourage the use of the standards and/or specifications referred to in paragraph 1, for the provision of services, technical interfaces and/or network functions, to the extent strictly necessary to ensure interoperability of services and to improve freedom of choice for users.

   As long as standards and/or specifications have not been published in accordance with paragraph 1, Member States shall encourage the implementation of standards and/or specifications adopted by the European standards organisations.

   In the absence of such standards and/or specifications, Member States shall encourage the implementation of international standards or recommendations adopted by the International Telecommunication Union (ITU), the International Organisation for Standardisation (ISO) or the International Electrotechnical Commission (IEC).

   Where international standards exist, Member States shall encourage the European standards organisations to use them, or the relevant parts of them, as a basis for the standards they develop, except where such international standards or relevant parts would be ineffective.

3. If the standards and/or specifications referred to in paragraph 1 have not been adequately implemented so that interoperability of services in one or more Member States cannot be ensured, the implementation of such standards and/or specifications may be made compulsory under the procedure laid down in paragraph 4, to the extent strictly necessary to ensure such interoperability and to improve freedom of choice for users.

4. implementation of certain standards and/or specifications compulsory, it shall publish a notice in the Official Journal of the European Communities and invite public comment by all parties concerned. The Commission, acting in accordance with the procedure referred to in Article 22(3), shall make implementation of the relevant standards compulsory by making reference to them as compulsory standards in the list of standards and/or specifications published in the Official Journal of the European Communities.

5. Where the Commission considers that standards and/or specifications referred to in paragraph 1 no longer contribute to the provision of harmonised electronic communications services, or that they no longer meet consumers' needs or are hampering technological development, it shall, acting in accordance with the procedure referred to in Article 22(2), remove them from the list of standards and/or specifications referred to in paragraph 1.

6. Where the Commission considers that standards and/or specifications referred to in paragraph 4 no longer contribute to the provision of harmonised electronic communications services, or that they no longer meet consumers' needs or are hampering technological development, it shall, acting in accordance with the procedure referred to in Article 22(3), remove them from this list of standards and/or specifications referred to in paragraph 1.

7. This Article does not apply in respect of any of the essential requirements, interface specifications or harmonised standards to which the provisions of Directive 1999/5/EC apply.

Article 18
Interoperability of digital interactive television services

1. In order to promote the free flow of information, media pluralism and cultural diversity, Member States shall encourage, in accordance with the provisions of Article 17(2):

   (a) providers of digital interactive television services for distribution to the public in the Community on digital interactive television platforms, regardless of the transmission mode, to use an open API;

   (b) providers of all enhanced digital television equipment deployed for the reception of digital interactive television services on interactive digital television platforms to comply with an open API in accordance with the minimum requirements of the relevant standards or specifications.

2. Without prejudice to Article 5(1)(b) of Directive 2002/19/ EC (Access Directive), Member States shall encourage proprietors of APIs to make available on fair, reasonable and non-discriminatory terms, and against appropriate remuneration, all such information as is necessary to enable providers of digital interactive television services to provide all services supported by the API in a fully functional form.

3. Within one year after the date of application referred to in Article 28(1), second subparagraph, the Commission shall examine the effects of this Article. If interoperability and freedom of choice for users have not been adequately achieved in one or more Member States, the Commission may take action in accordance with the procedure laid down in Article 17(3) and (4).

Article 19
Harmonisation procedures

1. Where the Commission, acting in accordance with the procedure referred to in Article 22(2), issues recommendations to Member States on the harmonised application of the provisions in this Directive and the Specific Directives in order to further the achievement of the objectives set out in Article 8, Member States shall ensure that national regulatory authorities take the utmost account of those recommendations in carrying out their tasks. Where a national regulatory authority chooses not to follow a recommendation, it shall inform the Commission giving the reasoning for its position.

2. Where the Commission finds that divergence at national level in regulations aimed at implementing Article 10(4) creates a barrier to the single market, the Commission may, acting in accordance with the procedure referred to in Article 22(3), take the appropriate technical implementing measures.

Article 20
Dispute resolution between undertakings

1. In the event of a dispute arising in connection with obligations arising under this Directive or the Specific Directives between undertakings providing electronic communications networks or services in a Member State, the national regulatory authority concerned shall, at the request of either party, and without prejudice to the provisions of paragraph 2, issue a binding decision to resolve the dispute in the shortest possible time frame and in any case within four months except in exceptional circumstances. The Member State concerned shall require that all parties cooperate fully with the national regulatory authority.

2. Member States may make provision for national regulatory authorities to decline to resolve a dispute through a binding decision where other mechanisms, including mediation, exist and would better contribute to resolution of the dispute in a timely manner in accordance with the provisions of Article 8. The national regulatory authority shall inform the parties without delay. If after four months the dispute is not resolved, and if the dispute has not been brought before the courts by the party seeking redress, the national regulatory authority shall issue, at the request of either party, a binding decision to resolve the dispute in the shortest possible time frame and in any case within four months.

3. In resolving a dispute, the national regulatory authority shall take decisions aimed at achieving the objectives set out in Article 8. Any obligations imposed on an undertaking by the national regulatory authority in resolving a dispute shall respect the provisions of this Directive or the Specific Directives.

4. The decision of the national regulatory authority shall be made available to the public, having regard to the requirements of business confidentiality. The parties concerned shall be given a full statement of the reasons on which it is based.

5. The procedure referred to in paragraphs 1, 3 and 4 shall not preclude either party from bringing an action before the courts.

Article 21
Resolution of cross-border disputes

1. In the event of a cross-border dispute arising under this Directive or the Specific Directives between parties in different Member States, where the dispute lies within the competence of national regulatory authorities from more than one Member State, the procedure set out in paragraphs 2, 3 and 4 shall be applicable.

2. Any party may refer the dispute to the national regulatory authorities concerned. The national regulatory authorities shall coordinate their efforts in order to bring about a resolution of the dispute, in accordance with the objectives set out in Article 8. Any obligations imposed on an undertaking by the national regulatory authority in resolving a dispute shall respect the provisions of this Directive or the Specific Directives.

3. Member States may make provision for national regulatory authorities jointly to decline to resolve a dispute where other mechanisms, including mediation, exist and would better contribute to resolution of the dispute in a timely manner in accordance with the provisions of Article 8. They shall inform the parties without delay. If after four months the dispute is not resolved, if the dispute has not been brought be-

fore the courts by the party seeking redress, and if either party requests it, the national regulatory authorities shall coordinate their efforts in order to bring about a resolution of the dispute, in accordance with the provisions set out in Article 8.

4. The procedure referred to in paragraph 2 shall not preclude either party from bringing an action before the courts.

Article 22
Committee

1. The Commission shall be assisted by a Committee ("the Communications Committee").

2. Where reference is made to this paragraph, Articles 3 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

3. Where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

   The period laid down in Article 5(6) of Decision 1999/468/EC shall be three months.

4. The Committee shall adopt its rules of procedure.

Article 23
Exchange of information

1. The Commission shall provide all relevant information to the Communications Committee on the outcome of regular consultations with the representatives of network operators, service providers, users, consumers, manufacturers and trade unions, as well as third countries and international organisations.

2. The Communications Committee shall, taking account of the Community's electronic communications policy, foster the exchange of information between the Member States and between the Member States and the Commission on the situation and the development of regulatory activities regarding electronic communications networks and services.

Article 24
Publication of information

1. Member States shall ensure that up-to-date information pertaining to the application of this Directive and the Specific Directives is made publicly available in a manner that guarantees all interested parties easy access to that information. They shall publish a notice in their national official gazette describing how and where the information is published. The first such notice shall be published before the date of application referred to in Article 28(1), second subparagraph, and thereafter a notice shall be published whenever there is any change in the information contained therein.

2. Member States shall send to the Commission a copy of all such notices at the time of publication. The Commission shall distribute the information to the Communications Committee as appropriate.

Article 25
Review procedures

1. The Commission shall periodically review the functioning of this Directive and report to the European Parliament and to the Council, on the first occasion not later than three years after the date of application referred to in Article 28(1), second subparagraph. For this purpose, the Commission may request information from the Member States, which shall be supplied without undue delay.

CHAPTER V
FINAL PROVISIONS

Article 26
Repeal

The following Directives and Decisions are hereby repealed with effect from the date of application referred to in Article 28(1), second subparagraph:

- Directive 90/387/EEC,
- Council Decision 91/396/EEC of 29 July 1991 on the introduction of a single European emergency call number(21),
- Council Directive 92/44/EEC of 5 June 1992 on the application of open network provision to leased lines(22),
- Council Decision 92/264/EEC of 11 May 1992 on the introduction of a standard international telephone access code in the Community(23),
- Directive 95/47/EC,
- Directive 97/13/EC,
- Directive 97/33/EC,

- Directive 98/10/EC of the European Parliament and of the Council of 26 February 1998 on the application of open network provision (ONP) to voice telephony and on universal service for telecommunications in a competitive environment(24).

Article 27
Transitional measures

Member States shall maintain all obligations under national law referred to in Article 7 of Directive 2002/19/EC (Access Directive) and Article 16 of Directive 2002/22/EC (Universal Service Directive) until such time as a determination is made in respect of those obligations by a national regulatory authority in accordance with Article 16 of this Directive.

Operators of fixed public telephone networks that were designated by their national regulatory authority as having significant market power in the provision of fixed public telephone networks and services under Annex I, Part 1 of Directive 97/33/EC or Directive 98/10/EC shall continue to be considered "notified operators" for the purposes of Regulation (EC) No 2887/2000 until such a time as the market analysis procedure referred to in Article 16 has been completed. Thereafter they shall cease to be considered "notified operators" for the purposes of the Regulation.

Article 28
Transposition

1. Member States shall adopt and publish the laws, regulations and administrative provisions necessary to comply with this Directive not later than 24 July 2003. They shall forthwith inform the Commission thereof.

   They shall apply those measures from 25 July 2003.

2. When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such a reference shall be laid down by the Member States.

3. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive and of any subsequent amendments to those provisions.

Article 29
Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 30
Addressees

This Directive is addressed to the Member States.

Done at Brussels, 7 March 2002.
For the European Parliament
The President P. Cox
For the Council
The President J. C. Aparicio

[1] OJ C 365 E, 19.12.2000, p. 198 and OJ C 270 E, 25.9.2001, p. 199.

[2] OJ C 123, 25.4.2001, p. 56.

[3] Opinion of the European Parliament of 1 March 2001 (OJ C 277, 1.10.2001, p. 91), Council Common Position of 17 September 2001 (OJ C 337, 30.11.2001, p. 34) and Decision of the European Parliament of 12 December 2001 (not yet published in the Official Journal). Council Decision of 14 February 2002.

[4] OJ L 192, 24.7.1990, p. 1. Directive as amended by Directive 97/51/EC of the European Parliament and of the Council (OJ L 295, 29.10.1997, p. 23).

[5] See page 21 of this Official Journal.

[6] See page 7 of this Official Journal.

[7] See page 51 of this Official Journal.

[8] OJ L 24, 30.1.1998, p. 1.

[9] OJ L 298, 17.10.1989, p. 23. Directive as amended by Directive 97/36/EC of the European Parliament and of the Council (OJ L 202, 30.7.1997, p. 60).

[10] OJ L 91, 7.4.1999, p. 10.

[11] OJ L 178, 17.7.2000, p. 1.

[12] OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).

[13] See page 1 of this Official Journal.

[14] OJ L 199, 26.7.1997, p. 32. Directive as amended by Directive 98/61/EC (OJ L 268, 3.10.1998, p. 37).

[15] OJ L 281, 23.11.1995, p. 51.

[16] OJ L 77, 26.3.1973, p. 29.

[17] OJ L 139, 23.5.1989, p. 19.

[18] OJ L 117, 7.5.1997, p. 15.

[19] OJ L 184, 17.7.1999, p. 23.

[20] OJ L 336, 30.12.2000, p. 4.

[21] OJ L 217, 6.8.1991, p. 31.

[22] OJ L 165, 19.6.1992, p. 27. Directive as last amended by Commission Decision 98/80/EC (OJ L 14, 20.1.1998, p. 27).

[23] OJ L 137, 20.5.1992, p. 21.

[24] OJ L 101, 1.4.1998, p. 24.

ANNEX I

List of markets to be included in the initial Commission recommendation on relevant product and service markets referred to in Article 15

1. Markets referred to in Directive 2002/22/EC (Universal Service Directive)

   Article 16 - Markets defined under the former regulatory framework, where obligations should be reviewed.

   The provision of connection to and use of the public telephone network at fixed locations.

   The provision of leased lines to end users.

2. Markets referred to in Directive 2002/19/EC (Access Directive)

Article 7 - Markets defined under the former regulatory framework, where obligations should be reviewed.

Interconnection (Directive 97/33/EC)

call origination in the fixed public telephone network

call termination in the fixed public telephone network

transit services in the fixed public telephone network

call origination on public mobile telephone networks

call termination on public mobile telephone networks

leased line interconnection (interconnection of part circuits)

Network access and special network access (Directive 97/33/EC, Directive 98/10/EC)

access to the fixed public telephone network, including unbundled access to the local loop

access to public mobile telephone networks, including carrier selection

Wholesale leased line capacity (Directive 92/44/EEC)

wholesale provision of leased line capacity to other suppliers of electronic communications networks or services

3. Markets referred to in Regulation (EC) No 2887/2000

   Services provided over unbundled (twisted metallic pair) loops.

4. Additional markets

   The national market for international roaming services on public mobile telephone networks.

ANNEX II

Criteria to be used by national regulatory authorities in making an assessment of joint dominance in accordance with Article 14(2), second subparagraph

Two or more undertakings can be found to be in a joint dominant position within the meaning of Article 14 if, even in the absence of structural or other links between them, they operate in a market the structure of which is considered to be conducive to coordinated effects. Without prejudice to the case law of the Court of Justice on joint dominance, this is likely to be the case where the market satisfies a number of appropriate characteristics, in particular in terms of market concentration, transparency and other characteristics mentioned below:

- mature market,
- stagnant or moderate growth on the demand side,
- low elasticity of demand,
- homogeneous product,
- similar cost structures,
- similar market shares,
- lack of technical innovation, mature technology,
- absence of excess capacity,
- high barriers to entry,
- lack of countervailing buying power,
- lack of potential competition,
- various kinds of informal or other links between the undertakings concerned,

- retaliatory mechanisms,
- lack or reduced scope for price competition.

The above is not an exhaustive list, nor are the criteria cumulative. Rather, the list is intended to illustrate only the sorts of evidence that could be used to support assertions concerning the existence of joint dominance.

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission(1),

Having regard to the opinion of the Economic and Social Committee(2),

Having regard to the opinion of the Committee of the Regions(3),

Acting in accordance with the procedure laid down in Article 251 of the Treaty(4),

Whereas:

(1) The liberalisation of the telecommunications sector and increasing competition and choice for communications services go hand in hand with parallel action to create a harmonised regulatory framework which secures the delivery of universal service. The concept of universal service should evolve to reflect advances in technology, market developments and changes in user demand. The regulatory framework established for the full liberalisation of the telecommunications market in 1998 in the Community defined the minimum scope of universal service obligations and established rules for its costing and financing.

(2) Under Article 153 of the Treaty, the Community is to contribute to the protection of consumers.

(3) The Community and its Member States have undertaken commitments on the regulatory

framework of telecommunications networks and services in the context of the World Trade Organisation (WTO) agreement on basic telecommunications. Any member of the WTO has the right to define the kind of universal service obligation it wishes to maintain. Such obligations will not be regarded as anti-competitive per se, provided they are administered in a transparent, non-discriminatory and competitively neutral manner and are not more burdensome than necessary for the kind of universal service defined by the member.

(4) Ensuring universal service (that is to say, the provision of a defined minimum set of services to all end-users at an affordable price) may involve the provision of some services to some end-users at prices that depart from those resulting from normal market conditions. However, compensating undertakings designated to provide such services in such circumstances need not result in any distortion of competition, provided that designated undertakings are compensated for the specific net cost involved and provided that the net cost burden is recovered in a competitively neutral way.

(5) In a competitive market, certain obligations should apply to all undertakings providing publicly available telephone services at fixed locations and others should apply only to undertakings enjoying significant market power or which have been designated as a universal service operator.

(6) The network termination point represents a boundary for regulatory purposes between the regulatory framework for electronic communication networks and services and the regulation of telecommunication terminal equipment. Defining the location of the network termination point is the responsibility of the national regulatory authority, where necessary on the basis of a proposal by the relevant undertakings.

(7) Member States should continue to ensure that the services set out in Chapter II are made available with the quality specified to all end-users in their territory, irrespective of their geographical location, and, in the light of specific national conditions, at an affordable price. Member States may, in the context of universal service obligations and in the light of national conditions, take specific measures for consumers in rural or geographically isolated areas to ensure their access to the services set out in the Chapter II and the affordability of those services, as well as ensure under the same conditions this access, in particular for the elderly, the disabled and for people with special social needs. Such measures may also include measures directly targeted at consumers with special social needs providing support to identified consumers, for example by means of specific measures, taken after the examination of individual requests, such as the paying off of debts.

(8) A fundamental requirement of universal service is to provide users on request with a connection to the public telephone network at a fixed location, at an affordable price. The requirement is limited to a single narrowband network connection, the provision of which may be restricted by Member States to the end-user's primary location/residence, and does not extend to the Integrated Services Digital Network (ISDN) which provides two or more connections capable of being used simultaneously. There should be no constraints on the technical means by which the connection is provided, allowing for wired or wireless technologies, nor any constraints on which operators provide part or all of universal service obligations. Connections to the public telephone network at a fixed location should be capable of supporting speech and data communications at rates sufficient for access to online services such as those provided via the public Internet. The speed of Internet access experienced by a given user may depend on a number of factors including the provider(s) of Internet connectivity as well as the given application for which a connection is being used. The data rate that can be supported by a single narrowband connection to the public telephone network depends on the capabilities of the subscriber's terminal equipment as well as the connection. For this reason it is not appropriate to mandate a specific data or bit rate at Community level. Currently available voice band modems typically offer a data rate of 56 kbit/s and employ automatic data rate adaptation to cater for variable line quality, with the result that the achieved data rate may be lower than 56 kbit/s. Flexibility is required on the one hand to allow Member States to take measures where necessary to ensure that connections are capable of supporting such a data rate, and on the other hand to allow Member States where relevant to permit data rates below this upper limit of 56 kbits/s in order, for example, to exploit the capabilities of wireless technologies (including cellular wireless networks) to deliver universal service to a higher proportion of the population. This may be of particular importance in some accession countries where household

penetration of traditional telephone connections remains relatively low. In specific cases where the connection to the public telephony network at a fixed location is clearly insufficient to support satisfactory Internet access, Member States should be able to require the connection to be brought up to the level enjoyed by the majority of subscribers so that it supports data rates sufficient for access to the Internet. Where such specific measures produce a net cost burden for those consumers concerned, the net effect may be included in any net cost calculation of universal service obligations.

(9) The provisions of this Directive do not preclude Member States from designating different undertakings to provide the network and service elements of universal service. Designated undertakings providing network elements may be required to ensure such construction and maintenance as are necessary and proportionate to meet all reasonable requests for connection at a fixed location to the public telephone network and for access to publicly available telephone services at a fixed location.

(10) Affordable price means a price defined by Member States at national level in the light of specific national conditions, and may involve setting common tariffs irrespective of location or special tariff options to deal with the needs of low-income users. Affordability for individual consumers is related to their ability to monitor and control their expenditure.

(11) Directory information and a directory enquiry service constitute an essential access tool for publicly available telephone services and form part of the universal service obligation. Users and consumers desire comprehensive directories and a directory enquiry service covering all listed telephone subscribers and their numbers (including fixed and mobile numbers) and want this information to be presented in a non-preferential fashion. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(5) ensures the subscribers' right to privacy with regard to the inclusion of their personal information in a public directory.

(12) For the citizen, it is important for there to be adequate provision of public pay telephones, and for users to be able to call emergency telephone numbers and, in particular, the single European emergency call number ("112") free of charge from any telephone, including public pay telephones, without the use of any means of payment. Insufficient information about the existence of "112" deprives citizens of the additional safety ensured by the existence of this number at European level especially during their travel in other Member States.

(13) Member States should take suitable measures in order to guarantee access to and affordability of all publicly available telephone services at a fixed location for disabled users and users with special social needs. Specific measures for disabled users could include, as appropriate, making available accessible public telephones, public text telephones or equivalent measures for deaf or speech-impaired people, providing services such as directory enquiry services or equivalent measures free of charge for blind or partially sighted people, and providing itemised bills in alternative format on request for blind or partially sighted people. Specific measures may also need to be taken to enable disabled users and users with special social needs to access emergency services "112" and to give them a similar possibility to choose between different operators or service providers as other consumers. Quality of service standards have been developed for a range of parameters to assess the quality of services received by subscribers and how well undertakings designated with universal service obligations perform in achieving these standards. Quality of service standards do not yet exist in respect of disabled users. Performance standards and relevant parameters should be developed for disabled users and are provided for in Article 11 of this Directive. Moreover, national regulatory authorities should be enabled to require publication of quality of service performance data if and when such standards and parameters are developed. The provider of universal service should not take measures to prevent users from benefiting fully from services offered by different operators or service providers, in combination with its own services offered as part of universal service.

(14) The importance of access to and use of the public telephone network at a fixed location is such that it should be available to anyone reasonably requesting it. In accordance with the principle of subsidiarity, it is for Member States to decide on the basis of objective criteria which undertakings have universal service obligations for the purposes of this Directive, where appropriate taking into account the ability and the willingness of undertakings to accept all or part of the universal service obligations. It is im-

portant that universal service obligations are fulfilled in the most efficient fashion so that users generally pay prices that correspond to efficient cost provision. It is likewise important that universal service operators maintain the integrity of the network as well as service continuity and quality. The development of greater competition and choice provide more possibilities for all or part of the universal service obligations to be provided by undertakings other than those with significant market power. Therefore, universal service obligations could in some cases be allocated to operators demonstrating the most cost-effective means of delivering access and services, including by competitive or comparative selection procedures. Corresponding obligations could be included as conditions in authorisations to provide publicly available services.

(15) Member States should monitor the situation of consumers with respect to their use of publicly available telephone services and in particular with respect to affordability. The affordability of telephone service is related to the information which users receive regarding telephone usage expenses as well as the relative cost of telephone usage compared to other services, and is also related to their ability to control expenditure. Affordability therefore means giving power to consumers through obligations imposed on undertakings designated as having universal service obligations. These obligations include a specified level of itemised billing, the possibility for consumers selectively to block certain calls (such as high-priced calls to premium services), the possibility for consumers to control expenditure via pre-payment means and the possibility for consumers to offset up-front connection fees. Such measures may need to be reviewed and changed in the light of market developments. Current conditions do not warrant a requirement for operators with universal service obligations to alert subscribers where a predetermined limit of expenditure is exceeded or an abnormal calling pattern occurs. Review of the relevant legislative provisions in future should consider whether there is a possible need to alert subscribers for these reasons.

(16) Except in cases of persistent late payment or non-payment of bills, consumers should be protected from immediate disconnection from the network on the grounds of an unpaid bill and, particularly in the case of disputes over high bills for premium rate services, should continue to have access to essential telephone services pending resolution of the dispute. Member States may decide that such access may continue to be provided only if the subscriber continues to pay line rental charges.

(17) Quality and price are key factors in a competitive market and national regulatory authorities should be able to monitor achieved quality of service for undertakings which have been designated as having universal service obligations. In relation to the quality of service attained by such undertakings, national regulatory authorities should be able to take appropriate measures where they deem it necessary. National regulatory authorities should also be able to monitor the achieved quality of services of other undertakings providing public telephone networks and/or publicly available telephone services to users at fixed locations.

(18) Member States should, where necessary, establish mechanisms for financing the net cost of universal service obligations in cases where it is demonstrated that the obligations can only be provided at a loss or at a net cost which falls outside normal commercial standards. It is important to ensure that the net cost of universal service obligations is properly calculated and that any financing is undertaken with minimum distortion to the market and to undertakings, and is compatible with the provisions of Articles 87 and 88 of the Treaty.

(19) Any calculation of the net cost of universal service should take due account of costs and revenues, as well as the intangible benefits resulting from providing universal service, but should not hinder the general aim of ensuring that pricing structures reflect costs. Any net costs of universal service obligations should be calculated on the basis of transparent procedures.

(20) Taking into account intangible benefits means that an estimate in monetary terms, of the indirect benefits that an undertaking derives by virtue of its position as provider of universal service, should be deducted from the direct net cost of universal service obligations in order to determine the overall cost burden.

(21) When a universal service obligation represents an unfair burden on an undertaking, it is appropriate to allow Member States to establish mechanisms for efficiently recovering net costs. Recovery via public funds constitutes one method of recovering the net costs of universal service obligations. It is also reasonable for established net costs to be recovered from all users in a transparent fashion by means of levies on undertakings. Member States should be able

to finance the net costs of different elements of universal service through different mechanisms, and/or to finance the net costs of some or all elements from either of the mechanisms or a combination of both. In the case of cost recovery by means of levies on undertakings, Member States should ensure that that the method of allocation amongst them is based on objective and non-discriminatory criteria and is in accordance with the principle of proportionality. This principle does not prevent Member States from exempting new entrants which have not yet achieved any significant market presence. Any funding mechanism should ensure that market participants only contribute to the financing of universal service obligations and not to other activities which are not directly linked to the provision of the universal service obligations. Recovery mechanisms should in all cases respect the principles of Community law, and in particular in the case of sharing mechanisms those of non-discrimination and proportionality. Any funding mechanism should ensure that users in one Member State do not contribute to universal service costs in another Member State, for example when making calls from one Member State to another.

(22) Where Member States decide to finance the net cost of universal service obligations from public funds, this should be understood to comprise funding from general government budgets including other public financing sources such as state lotteries.

(23) The net cost of universal service obligations may be shared between all or certain specified classes of undertaking. Member States should ensure that the sharing mechanism respects the principles of transparency, least market distortion, non-discrimination and proportionality. Least market distortion means that contributions should be recovered in a way that as far as possible minimises the impact of the financial burden falling on end-users, for example by spreading contributions as widely as possible.

(24) National regulatory authorities should satisfy themselves that those undertakings benefiting from universal service funding provide a sufficient level of detail of the specific elements requiring such funding in order to justify their request. Member States' schemes for the costing and financing of universal service obligations should be communicated to the Commission for verification of compatibility with the Treaty. There are incentives for designated operators to raise the assessed net cost of universal service obligations. Therefore Member States should ensure effective transparency and control of amounts charged to finance universal service obligations.

(25) Communications markets continue to evolve in terms of the services used and the technical means used to deliver them to users. The universal service obligations, which are defined at a Community level, should be periodically reviewed with a view to proposing that the scope be changed or redefined. Such a review should take account of evolving social, commercial and technological conditions and the fact that any change of scope should be subject to the twin test of services that become available to a substantial majority of the population, with a consequent risk of social exclusion for those who can not afford them. Care should be taken in any change of the scope of universal service obligations to ensure that certain technological choices are not artificially promoted above others, that a disproportionate financial burden is not imposed on sector undertakings (thereby endangering market developments and innovation) and that any financing burden does not fall unfairly on consumers with lower incomes. Any change of scope automatically means that any net cost can be financed via the methods permitted in this Directive. Member States are not permitted to impose on market players financial contributions which relate to measures which are not part of universal service obligations. Individual Member States remain free to impose special measures (outside the scope of universal service obligations) and finance them in conformity with Community law but not by means of contributions from market players.

(26) More effective competition across all access and service markets will give greater choice for users. The extent of effective competition and choice varies across the Community and varies within Member States between geographical areas and between access and service markets. Some users may be entirely dependent on the provision of access and services by an undertaking with significant market power. In general, for reasons of efficiency and to encourage effective competition, it is important that the services provided by an undertaking with significant market power reflect costs. For reasons of efficiency and social reasons, end-user tariffs should reflect demand conditions as well as cost conditions, provided that this does not result in distortions of competition. There is a risk that an undertaking with significant market power may act in various ways to inhibit entry

or distort competition, for example by charging excessive prices, setting predatory prices, compulsory bundling of retail services or showing undue preference to certain customers. Therefore, national regulatory authorities should have powers to impose, as a last resort and after due consideration, retail regulation on an undertaking with significant market power. Price cap regulation, geographical averaging or similar instruments, as well as non-regulatory measures such as publicly available comparisons of retail tariffs, may be used to achieve the twin objectives of promoting effective competition whilst pursuing public interest needs, such as maintaining the affordability of publicly available telephone services for some consumers. Access to appropriate cost accounting information is necessary, in order for national regulatory authorities to fulfil their regulatory duties in this area, including the imposition of any tariff controls. However, regulatory controls on retail services should only be imposed where national regulatory authorities consider that relevant wholesale measures or measures regarding carrier selection or pre-selection would fail to achieve the objective of ensuring effective competition and public interest.

(27) Where a national regulatory authority imposes obligations to implement a cost accounting system in order to support price controls, it may itself undertake an annual audit to ensure compliance with that cost accounting system, provided that it has the necessary qualified staff, or it may require the audit to be carried out by another qualified body, independent of the operator concerned.

(28) It is considered necessary to ensure the continued application of the existing provisions relating to the minimum set of leased line services in Community telecommunications legislation, in particular in Council Directive 92/44/EEC of 5 June 1992 on the application of open network provision to leased lines(6), until such time as national regulatory authorities determine, in accordance with the market analysis procedures laid down in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)(7), that such provisions are no longer needed because a sufficiently competitive market has developed in their territory. The degree of competition is likely to vary between different markets of leased lines in the minimum set, and in different parts of the territory. In undertaking the market analysis, national regulatory authorities should make separate assessments for each market of leased lines in the minimum set, taking into account their geographic dimension. Leased lines services constitute mandatory services to be provided without recourse to any compensation mechanisms. The provision of leased lines outside of the minimum set of leased lines should be covered by general retail regulatory provisions rather than specific requirements covering the supply of the minimum set.

(29) National regulatory authorities may also, in the light of an analysis of the relevant market, require mobile operators with significant market power to enable their subscribers to access the services of any interconnected provider of publicly available telephone services on a call-by-call basis or by means of pre-selection.

(30) Contracts are an important tool for users and consumers to ensure a minimum level of transparency of information and legal security. Most service providers in a competitive environment will conclude contracts with their customers for reasons of commercial desirability. In addition to the provisions of this Directive, the requirements of existing Community consumer protection legislation relating to contracts, in particular Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts(8) and Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts(9), apply to consumer transactions relating to electronic networks and services. Specifically, consumers should enjoy a minimum level of legal certainty in respect of their contractual relations with their direct telephone service provider, such that the contractual terms, conditions, quality of service, condition for termination of the contract and the service, compensation measures and dispute resolution are specified in their contracts. Where service providers other than direct telephone service providers conclude contracts with consumers, the same information should be included in those contracts as well. The measures to ensure transparency on prices, tariffs, terms and conditions will increase the ability of consumers to optimise their choices and thus to benefit fully from competition.

(31) End-users should have access to publicly available information on communications services. Member States should be able to monitor the quality of services which are offered in their territories. National regulatory authorities should

be able systematically to collect information on the quality of services offered in their territories on the basis of criteria which allow comparability between service providers and between Member States. Undertakings providing communications services, operating in a competitive environment, are likely to make adequate and up-to-date information on their services publicly available for reasons of commercial advantage. National regulatory authorities should nonetheless be able to require publication of such information where it is demonstrated that such information is not effectively available to the public.

(32) End-users should be able to enjoy a guarantee of interoperability in respect of all equipment sold in the Community for the reception of digital television. Member States should be able to require minimum harmonised standards in respect of such equipment. Such standards could be adapted from time to time in the light of technological and market developments.

(33) It is desirable to enable consumers to achieve the fullest connectivity possible to digital television sets. Interoperability is an evolving concept in dynamic markets. Standards bodies should do their utmost to ensure that appropriate standards evolve along with the technologies concerned. It is likewise important to ensure that connectors are available on television sets that are capable of passing all the necessary elements of a digital signal, including the audio and video streams, conditional access information, service information, application program interface (API) information and copy protection information. This Directive therefore ensures that the functionality of the open interface for digital television sets is not limited by network operators, service providers or equipment manufacturers and continues to evolve in line with technological developments. For display and presentation of digital interactive television services, the realisation of a common standard through a market-driven mechanism is recognised as a consumer benefit. Member States and the Commission may take policy initiatives, consistent with the Treaty, to encourage this development.

(34) All end-users should continue to enjoy access to operator assistance services whatever organisation provides access to the public telephone network.

(35) The provision of directory enquiry services and directories is already open to competition. The provisions of this Directive complement the provisions of Directive 97/66/EC by giving subscribers a right to have their personal data included in a printed or electronic directory. All service providers which assign telephone numbers to their subscribers are obliged to make relevant information available in a fair, cost-oriented and non-discriminatory manner.

(36) It is important that users should be able to call the single European emergency number "112", and any other national emergency telephone numbers, free of charge, from any telephone, including public pay telephones, without the use of any means of payment. Member States should have already made the necessary organisational arrangements best suited to the national organisation of the emergency systems, in order to ensure that calls to this number are adequately answered and handled. Caller location information, to be made available to the emergency services, will improve the level of protection and the security of users of "112" services and assist the emergency services, to the extent technically feasible, in the discharge of their duties, provided that the transfer of calls and associated data to the emergency services concerned is guaranteed. The reception and use of such information should comply with relevant Community law on the processing of personal data. Steady information technology improvements will progressively support the simultaneous handling of several languages over the networks at a reasonable cost. This in turn will ensure additional safety for European citizens using the "112" emergency call number.

(37) Easy access to international telephone services is vital for European citizens and European businesses. "00" has already been established as the standard international telephone access code for the Community. Special arrangements for making calls between adjacent locations across borders between Member States may be established or continued. The ITU has assigned, in accordance with ITU Recommendation E.164, code "3883" to the European Telephony Numbering Space (ETNS). In order to ensure connection of calls to the ETNS, undertakings operating public telephone networks should ensure that calls using "3883" are directly or indirectly interconnected to ETNS serving networks specified in the relevant European Telecommunications Standards Institute (ETSI) standards. Such interconnection arrangements should be governed by the provisions of Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection

of, electronic communications networks and associated facilities (Access Directive)(10).

(38) Access by end-users to all numbering resources in the Community is a vital pre-condition for a single market. It should include freephone, premium rate, and other non-geographic numbers, except where the called subscriber has chosen, for commercial reasons, to limit access from certain geographical areas. Tariffs charged to parties calling from outside the Member State concerned need not be the same as for those parties calling from inside that Member State.

(39) Tone dialling and calling line identification facilities are normally available on modern telephone exchanges and can therefore increasingly be provided at little or no expense. Tone dialling is increasingly being used for user interaction with special services and facilities, including value added services, and the absence of this facility can prevent the user from making use of these services. Member States are not required to impose obligations to provide these facilities when they are already available. Directive 97/66/EC safeguards the privacy of users with regard to itemised billing, by giving them the means to protect their right to privacy when calling line identification is implemented. The development of these services on a pan-European basis would benefit consumers and is encouraged by this Directive.

(40) Number portability is a key facilitator of consumer choice and effective competition in a competitive telecommunications environment such that end-users who so request should be able to retain their number(s) on the public telephone network independently of the organisation providing service. The provision of this facility between connections to the public telephone network at fixed and non-fixed locations is not covered by this Directive. However, Member States may apply provisions for porting numbers between networks providing services at a fixed location and mobile networks.

(41) The impact of number portability is considerably strengthened when there is transparent tariff information, both for end-users who port their numbers and also for end-users who call those who have ported their numbers. National regulatory authorities should, where feasible, facilitate appropriate tariff transparency as part of the implementation of number portability.

(42) When ensuring that pricing for interconnection related to the provision of number portability is cost-oriented, national regulatory authorities may also take account of prices available in comparable markets.

(43) Currently, Member States impose certain "must carry" obligations on networks for the distribution of radio or television broadcasts to the public. Member States should be able to lay down proportionate obligations on undertakings under their jurisdiction, in the interest of legitimate public policy considerations, but such obligations should only be imposed where they are necessary to meet general interest objectives clearly defined by Member States in conformity with Community law and should be proportionate, transparent and subject to periodical review. "Must carry" obligations imposed by Member States should be reasonable, that is they should be proportionate and transparent in the light of clearly defined general interest objectives, and could, where appropriate, entail a provision for proportionate remuneration. Such "must carry" obligations may include the transmission of services specifically designed to enable appropriate access by disabled users.

(44) Networks used for the distribution of radio or television broadcasts to the public include cable, satellite and terrestrial broadcasting networks. They might also include other networks to the extent that a significant number of end-users use such networks as their principal means to receive radio and television broadcasts.

(45) Services providing content such as the offer for sale of a package of sound or television broadcasting content are not covered by the common regulatory framework for electronic communications networks and services. Providers of such services should not be subject to universal service obligations in respect of these activities. This Directive is without prejudice to measures taken at national level, in compliance with Community law, in respect of such services.

(46) Where a Member State seeks to ensure the provision of other specific services throughout its national territory, such obligations should be implemented on a cost efficient basis and outside the scope of universal service obligations. Accordingly, Member States may undertake additional measures (such as facilitating the development of infrastructure or services in circumstances where the market does not satisfactorily address the requirements of end-users or consumers), in conformity with Community law. As a reaction to the Commission's e-Europe initiative, the Lisbon European Council of 23 and 24

March 2000 called on Member States to ensure that all schools have access to the Internet and to multimedia resources.

(47) In the context of a competitive environment, the views of interested parties, including users and consumers, should be taken into account by national regulatory authorities when dealing with issues related to end-users' rights. Effective procedures should be available to deal with disputes between consumers, on the one hand, and undertakings providing publicly available communications services, on the other. Member States should take full account of Commission Recommendation 98/257/EC of 30 March 1998 on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes(11).

(48) Co-regulation could be an appropriate way of stimulating enhanced quality standards and improved service performance. Co-regulation should be guided by the same principles as formal regulation, i.e. it should be objective, justified, proportional, non-discriminatory and transparent.

(49) This Directive should provide for elements of consumer protection, including clear contract terms and dispute resolution, and tariff transparency for consumers. It should also encourage the extension of such benefits to other categories of end-users, in particular small and medium-sized enterprises.

(50) The provisions of this Directive do not prevent a Member State from taking measures justified on grounds set out in Articles 30 and 46 of the Treaty, and in particular on grounds of public security, public policy and public morality.

(51) Since the objectives of the proposed action, namely setting a common level of universal service for telecommunications for all European users and of harmonising conditions for access to and use of public telephone networks at a fixed location and related publicly available telephone services and also achieving a harmonised framework for the regulation of electronic communications services, electronic communications networks and associated facilities, cannot be sufficiently achieved by the Member States and can therefore by reason of the scale or effects of the action be better achieved at Community level, the Community may adopt measures in accordance with the principles of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(52) The measures necessary for the implementation of this Directive should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission(12),

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I
SCOPE, AIMS AND DEFINITIONS

Article 1
Scope and aims

1. Within the framework of Directive 2002/21/EC (Framework Directive), this Directive concerns the provision of electronic communications networks and services to end-users. The aim is to ensure the availability throughout the Community of good quality publicly available services through effective competition and choice and to deal with circumstances in which the needs of end-users are not satisfactorily met by the market.

2. This Directive establishes the rights of end-users and the corresponding obligations on undertakings providing publicly available electronic communications networks and services. With regard to ensuring provision of universal service within an environment of open and competitive markets, this Directive defines the minimum set of services of specified quality to which all end-users have access, at an affordable price in the light of specific national conditions, without distorting competition. This Directive also sets out obligations with regard to the provision of certain mandatory services such as the retail provision of leased lines.

Article 2
Definitions

For the purposes of this Directive, the definitions set out in Article 2 of Directive 2002/21/EC (Framework Directive) shall apply.

The following definitions shall also apply:

(a) "public pay telephone" means a telephone available to the general public, for the use of which the means of payment may include coins and/

or credit/debit cards and/or pre-payment cards, including cards for use with dialling codes;

(b) "public telephone network" means an electronic communications network which is used to provide publicly available telephone services; it supports the transfer between network termination points of speech communications, and also other forms of communication, such as facsimile and data;

(c) "publicly available telephone service" means a service available to the public for originating and receiving national and international calls and access to emergency services through a number or numbers in a national or international telephone numbering plan, and in addition may, where relevant, include one or more of the following services: the provision of operator assistance, directory enquiry services, directories, provision of public pay phones, provision of service under special terms, provision of special facilities for customers with disabilities or with special social needs and/or the provision of non-geographic services;

(d) "geographic number" means a number from the national numbering plan where part of its digit structure contains geographic significance used for routing calls to the physical location of the network termination point (NTP);

(e) "network termination point" (NTP) means the physical point at which a subscriber is provided with access to a public communications network; in the case of networks involving switching or routing, the NTP is identified by means of a specific network address, which may be linked to a subscriber number or name;

(f) "non-geographic numbers" means a number from the national numbering plan that is not a geographic number. It includes inter alia mobile, freephone and premium rate numbers.

CHAPTER II
UNIVERSAL SERVICE OBLIGATIONS INCLUDING SOCIAL OBLIGATIONS

Article 3
Availability of universal service

1. Member States shall ensure that the services set out in this Chapter are made available at the quality specified to all end-users in their territory, independently of geographical location, and, in the light of specific national conditions, at an affordable price.

2. Member States shall determine the most efficient and appropriate approach for ensuring the implementation of universal service, whilst respecting the principles of objectivity, transparency, non-discrimination and proportionality. They shall seek to minimise market distortions, in particular the provision of services at prices or subject to other terms and conditions which depart from normal commercial conditions, whilst safeguarding the public interest.

Article 4
Provision of access at a fixed location

1. Member States shall ensure that all reasonable requests for connection at a fixed location to the public telephone network and for access to publicly available telephone services at a fixed location are met by at least one undertaking.

2. The connection provided shall be capable of allowing end-users to make and receive local, national and international telephone calls, facsimile communications and data communications, at data rates that are sufficient to permit functional Internet access, taking into account prevailing technologies used by the majority of subscribers and technological feasibility.

Article 5
Directory enquiry services and directories

1. Member States shall ensure that:

   (a) at least one comprehensive directory is available to end-users in a form approved by the relevant authority, whether printed or electronic, or both, and is updated on a regular basis, and at least once a year;

   (b) at least one comprehensive telephone directory enquiry service is available to all end-users, including users of public pay telephones.

2. The directories in paragraph 1 shall comprise, subject to the provisions of Article 11 of Directive 97/66/EC, all subscribers of publicly available telephone services.

3. Member States shall ensure that the undertaking(s) providing the services referred to in paragraph 1 apply the principle of non-discrimination to the treatment of information that has been provided to them by other undertakings.

Article 6
Public pay telephones

1. Member States shall ensure that national regulatory authorities can impose obligations on undertakings in order to ensure that public pay telephones are provided to meet the reasonable needs of end-users in terms of the geographical coverage, the number of telephones, the accessibility of such telephones to disabled users and the quality of services.

2. A Member State shall ensure that its national regulatory authority can decide not to impose obligations under paragraph 1 in all or part of its territory, if it is satisfied that these facilities or comparable services are widely available, on the basis of a consultation of interested parties as referred to in Article 33.

3. Member States shall ensure that it is possible to make emergency calls from public pay telephones using the single European emergency call number "112" and other national emergency numbers, all free of charge and without having to use any means of payment.

Article 7
Special measures for disabled users

1. Member States shall, where appropriate, take specific measures for disabled end-users in order to ensure access to and affordability of publicly available telephone services, including access to emergency services, directory enquiry services and directories, equivalent to that enjoyed by other end-users.

2. Member States may take specific measures, in the light of national conditions, to ensure that disabled end-users can also take advantage of the choice of undertakings and service providers available to the majority of end-users.

Article 8
Designation of undertakings

1. Member States may designate one or more undertakings to guarantee the provision of universal service as identified in Articles 4, 5, 6 and 7 and, where applicable, Article 9(2) so that the whole of the national territory can be covered. Member States may designate different undertakings or sets of undertakings to provide different elements of universal service and/or to cover different parts of the national territory.

2. When Member States designate undertakings in part or all of the national territory as having universal service obligations, they shall do so using an efficient, objective, transparent and non-discriminatory designation mechanism, whereby no undertaking is a priori excluded from being designated. Such designation methods shall ensure that universal service is provided in a cost-effective manner and may be used as a means of determining the net cost of the universal service obligation in accordance with Article 12.

Article 9
Affordability of tariffs

1. National regulatory authorities shall monitor the evolution and level of retail tariffs of the services identified in Articles 4, 5, 6 and 7 as falling under the universal service obligations and provided by designated undertakings, in particular in relation to national consumer prices and income.

2. Member States may, in the light of national conditions, require that designated undertakings provide tariff options or packages to consumers which depart from those provided under normal commercial conditions, in particular to ensure that those on low incomes or with special social needs are not prevented from accessing or using the publicly available telephone service.

3. Member States may, besides any provision for designated undertakings to provide special tariff options or to comply with price caps or geographical averaging or other similar schemes, ensure that support is provided to consumers identified as having low incomes or special social needs.

4. Member States may require undertakings with obligations under Articles 4, 5, 6 and 7 to apply common tariffs, including geographical averaging, throughout the territory, in the light of national conditions or to comply with price caps.

5. National regulatory authorities shall ensure that, where a designated undertaking has an obligation to provide special tariff options, common tariffs, including geographical averaging, or to comply with price caps, the conditions are fully transparent and are published and applied in accordance with the principle of non-discrimination. National regulatory authorities may require that specific schemes be modified or withdrawn.

Article 10
Control of expenditure

1. Member States shall ensure that designated undertakings, in providing facilities and services additional to those referred to in Articles 4, 5, 6, 7 and 9(2), establish terms and conditions in such a way that the subscriber is not obliged to pay for facilities or services which are not necessary or not required for the service requested.

2. Member States shall ensure that designated undertakings with obligations under Articles 4, 5, 6, 7 and 9(2) provide the specific facilities and services set out in Annex I, Part A, in order that subscribers can monitor and control expenditure and avoid unwarranted disconnection of service.

3. Member States shall ensure that the relevant authority is able to waive the requirements of paragraph 2 in all or part of its national territory if it is satisfied that the facility is widely available.

Article 11
Quality of service of designated undertakings

1. National regulatory authorities shall ensure that all designated undertakings with obligations under Articles 4, 5, 6, 7 and 9(2) publish adequate and up-to-date information concerning their performance in the provision of universal service, based on the quality of service parameters, definitions and measurement methods set out in Annex III. The published information shall also be supplied to the national regulatory authority.

2. National regulatory authorities may specify, inter alia, additional quality of service standards, where relevant parameters have been developed, to assess the performance of undertakings in the provision of services to disabled end-users and disabled consumers. National regulatory authorities shall ensure that information concerning the performance of undertakings in relation to these parameters is also published and made available to the national regulatory authority.

3. National regulatory authorities may, in addition, specify the content, form and manner of information to be published, in order to ensure that end-users and consumers have access to comprehensive, comparable and user-friendly information.

4. National regulatory authorities shall be able to set performance targets for those undertakings with universal service obligations at least under Article 4. In so doing, national regulatory authorities shall take account of views of interested parties, in particular as referred to in Article 33.

5. Member States shall ensure that national regulatory authorities are able to monitor compliance with these performance targets by designated undertakings.

6. Persistent failure by an undertaking to meet performance targets may result in specific measures being taken in accordance with Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive)(13). National regulatory authorities shall be able to order independent audits or similar reviews of the performance data, paid for by the undertaking concerned, in order to ensure the accuracy and comparability of the data made available by undertakings with universal service obligations.

Article 12
Costing of universal service obligations

1. Where national regulatory authorities consider that the provision of universal service as set out in Articles 3 to 10 may represent an unfair burden on undertakings designated to provide universal service, they shall calculate the net costs of its provision.

   For that purpose, national regulatory authorities shall:

   (a) calculate the net cost of the universal service obligation, taking into account any market benefit which accrues to an undertaking designated to provide universal service, in accordance with Annex IV, Part A; or

   (b) make use of the net costs of providing universal service identified by a designation mechanism in accordance with Article 8(2).

2. The accounts and/or other information serving as the basis for the calculation of the net cost of universal service obligations under paragraph 1(a) shall be audited or verified by the national regulatory authority or a body independent of the relevant parties and approved by the national regulatory authority. The results of the cost calculation and the conclusions of the audit shall be publicly available.

Article 13
Financing of universal service obligations

1. Where, on the basis of the net cost calculation referred to in Article 12, national regulatory authorities find that an undertaking is subject to an unfair burden, Member States shall, upon request from a designated undertaking, decide:

   (a) to introduce a mechanism to compensate that undertaking for the determined net costs under transparent conditions from public funds; and/or

   (b) to share the net cost of universal service obligations between providers of electronic communications networks and services.

2. Where the net cost is shared under paragraph 1(b), Member States shall establish a sharing mechanism administered by the national regulatory authority or a body independent from the beneficiaries under the supervision of the national regulatory authority. Only the net cost, as determined in accordance with Article 12, of the obligations laid down in Articles 3 to 10 may be financed.

3. A sharing mechanism shall respect the principles of transparency, least market distortion, non-discrimination and proportionality, in accordance with the principles of Annex IV, Part B. Member States may choose not to require contributions from undertakings whose national turnover is less than a set limit.

4. Any charges related to the sharing of the cost of universal service obligations shall be unbundled and identified separately for each undertaking. Such charges shall not be imposed or collected from undertakings that are not providing services in the territory of the Member State that has established the sharing mechanism.

Article 14
Transparency

1. Where a mechanism for sharing the net cost of universal service obligations as referred to in Article 13 is established, national regulatory authorities shall ensure that the principles for cost sharing, and details of the mechanism used, are publicly available.

2. Subject to Community and national rules on business confidentiality, national regulatory authorities shall ensure that an annual report is published giving the calculated cost of universal service obligations, identifying the contributions made by all the undertakings involved, and identifying any market benefits, that may have accrued to the undertaking(s) designated to provide universal service, where a fund is actually in place and working.

Article 15
Review of the scope of universal service

1. The Commission shall periodically review the scope of universal service, in particular with a view to proposing to the European Parliament and the Council that the scope be changed or redefined. A review shall be carried out, on the first occasion within two years after the date of application referred to in Article 38(1), second subparagraph, and subsequently every three years.

2. This review shall be undertaken in the light of social, economic and technological developments, taking into account, inter alia, mobility and data rates in the light of the prevailing technologies used by the majority of subscribers. The review process shall be undertaken in accordance with Annex V. The Commission shall submit a report to the European Parliament and the Council regarding the outcome of the review.

CHAPTER III
REGULATORY CONTROLS ON UNDERTAKINGS WITH SIGNIFICANT MARKET POWER IN SPECIFIC MARKETS

Article 16
Review of obligations

1. Member States shall maintain all obligations relating to:

   (a) retail tariffs for the provision of access to and use of the public telephone network, imposed under Article 17 of Directive 98/10/EC of the European Parliament and of the Council of 26 February 1998 on the application of open network provision (ONP) to voice telephony and on universal service for telecommunications in a competitive environment(14);

   (b) carrier selection or pre-selection, imposed under Directive 97/33/EC of the European Parliament and of the Council of 30 June 1997 on interconnection in telecommunications with regard to ensuring universal

service and interoperability through application of the principles of open network provision (ONP)(15);

(c) leased lines, imposed under Articles 3, 4, 6, 7, 8 and 10 of Directive 92/44/EEC,

until a review has been carried out and a determination made in accordance with the procedure in paragraph 3 of this Article.

2. The Commission shall indicate relevant markets for the obligations relating to retail markets in the initial recommendation on relevant product and service markets and the Decision identifying transnational markets to be adopted in accordance with Article 15 of Directive 2002/21/EC (Framework Directive).

3. Member States shall ensure that, as soon as possible after the entry into force of this Directive, and periodically thereafter, national regulatory authorities undertake a market analysis, in accordance with the procedure set out in Article 16 of Directive 2002/21/EC (Framework Directive) to determine whether to maintain, amend or withdraw the obligations relating to retail markets. Measures taken shall be subject to the procedure referred to in Article 7 of Directive 2002/21/EC (Framework Directive).

Article 17
Regulatory controls on retail services

1. Member States shall ensure that, where:

(a) as a result of a market analysis carried out in accordance with Article 16(3) a national regulatory authority determines that a given retail market identified in accordance with Article 15 of Directive 2002/21/EC (Framework Directive) is not effectively competitive, and

(b) the national regulatory authority concludes that obligations imposed under Directive 2002/19/EC (Access Directive), or Article 19 of this Directive would not result in the achievement of the objectives set out in Article 8 of Directive 2002/21/EC (Framework Directive),

national regulatory authorities shall impose appropriate regulatory obligations on undertakings identified as having significant market power on a given retail market in accordance with Article 14 of Directive 2002/21/EC (Framework Directive).

2. Obligations imposed under paragraph 1 shall be based on the nature of the problem identified and be proportionate and justified in the light of the objectives laid down in Article 8 of Directive 2002/21/EC (Framework Directive). The obligations imposed may include requirements that the identified undertakings do not charge excessive prices, inhibit market entry or restrict competition by setting predatory prices, show undue preference to specific end-users or unreasonably bundle services. National regulatory authorities may apply to such undertakings appropriate retail price cap measures, measures to control individual tariffs, or measures to orient tariffs towards costs or prices on comparable markets, in order to protect end-user interests whilst promoting effective competition.

3. National regulatory authorities shall, on request, submit information to the Commission concerning the retail controls applied and, where appropriate, the cost accounting systems used by the undertakings concerned.

4. National regulatory authorities shall ensure that, where an undertaking is subject to retail tariff regulation or other relevant retail controls, the necessary and appropriate cost accounting systems are implemented. National regulatory authorities may specify the format and accounting methodology to be used. Compliance with the cost accounting system shall be verified by a qualified independent body. National regulatory authorities shall ensure that a statement concerning compliance is published annually.

5. Without prejudice to Article 9(2) and Article 10, national regulatory authorities shall not apply retail control mechanisms under paragraph 1 of this Article to geographical or user markets where they are satisfied that there is effective competition.

Article 18
Regulatory controls on the minimum set of leased lines

1. Where, as a result of the market analysis carried out in accordance with Article 16(3), a national regulatory authority determines that the market for the provision of part or all of the minimum set of leased lines is not effectively competitive, it shall identify undertakings with significant market power in the provision of those specific elements of the minimum set of leased lines services in all or part of its territory in accordance with Article 14 of Directive 2002/21/EC (Framework Directive). The national regulatory authority shall impose obligations regarding the provision of the minimum set of

leased lines, as identified in the list of standards published in the Official Journal of the European Communities in accordance with Article 17 of Directive 2002/21/EC (Framework Directive), and the conditions for such provision set out in Annex VII to this Directive, on such undertakings in relation to those specific leased line markets.

2. Where as a result of the market analysis carried out in accordance with Article 16(3), a national regulatory authority determines that a relevant market for the provision of leased lines in the minimum set is effectively competitive, it shall withdraw the obligations referred to in paragraph 1 in relation to this specific leased line market.

3. The minimum set of leased lines with harmonised characteristics, and associated standards, shall be published in the Official Journal of the European Communities as part of the list of standards referred to in Article 17 of Directive 2002/21/EC (Framework Directive). The Commission may adopt amendments necessary to adapt the minimum set of leased lines to new technical developments and to changes in market demand, including the possible deletion of certain types of leased line from the minimum set, acting in accordance with the procedure referred to in Article 37(2) of this Directive.

Article 19
Carrier selection and carrier pre-selection

1. National regulatory authorities shall require undertakings notified as having significant market power for the provision of connection to and use of the public telephone network at a fixed location in accordance with Article 16(3) to enable their subscribers to access the services of any interconnected provider of publicly available telephone services:

   (a) on a call-by-call basis by dialling a carrier selection code; and

   (b) by means of pre-selection, with a facility to override any pre-selected choice on a call-by-call basis by dialling a carrier selection code.

2. User requirements for these facilities to be implemented on other networks or in other ways shall be assessed in accordance with the market analysis procedure laid down in Article 16 of Directive 2002/21/EC (Framework Directive) and implemented in accordance with Article 12 of Directive 2002/19/EC (Access Directive).

3. National regulatory authorities shall ensure that pricing for access and interconnection related to the provision of the facilities in paragraph 1 is cost oriented and that direct charges to subscribers, if any, do not act as a disincentive for the use of these facilities.

CHAPTER IV
END-USER INTERESTS AND RIGHTS

Article 20
Contracts

1. Paragraphs 2, 3 and 4 apply without prejudice to Community rules on consumer protection, in particular Directives 97/7/EC and 93/13/EC, and national rules in conformity with Community law.

2. Member States shall ensure that, where subscribing to services providing connection and/or access to the public telephone network, consumers have a right to a contract with an undertaking or undertakings providing such services. The contract shall specify at least:

   (a) the identity and address of the supplier;

   (b) services provided, the service quality levels offered, as well as the time for the initial connection;

   (c) the types of maintenance service offered;

   (d) particulars of prices and tariffs and the means by which up-to-date information on all applicable tariffs and maintenance charges may be obtained;

   (e) the duration of the contract, the conditions for renewal and termination of services and of the contract;

   (f) any compensation and the refund arrangements which apply if contracted service quality levels are not met; and

   (g) the method of initiating procedures for settlement of disputes in accordance with Article 34.

   Member States may extend these obligations to cover other end-users.

3. Where contracts are concluded between consumers and electronic communications services providers other than those providing connection and/or access to the public telephone

network, the information in paragraph 2 shall also be included in such contracts. Member States may extend this obligation to cover other end-users.

4. Subscribers shall have a right to withdraw from their contracts without penalty upon notice of proposed modifications in the contractual conditions. Subscribers shall be given adequate notice, not shorter than one month, ahead of any such modifications and shall be informed at the same time of their right to withdraw, without penalty, from such contracts, if they do not accept the new conditions.

Article 21
Transparency and publication of information

1. Member States shall ensure that transparent and up-to-date information on applicable prices and tariffs, and on standard terms and conditions, in respect of access to and use of publicly available telephone services is available to end-users and consumers, in accordance with the provisions of Annex II.

2. National regulatory authorities shall encourage the provision of information to enable end-users, as far as appropriate, and consumers to make an independent evaluation of the cost of alternative usage patterns, by means of, for instance, interactive guides.

Article 22
Quality of service

1. Member States shall ensure that national regulatory authorities are, after taking account of the views of interested parties, able to require undertakings that provide publicly available electronic communications services to publish comparable, adequate and up-to-date information for end-users on the quality of their services. The information shall, on request, also be supplied to the national regulatory authority in advance of its publication.

2. National regulatory authorities may specify, inter alia, the quality of service parameters to be measured, and the content, form and manner of information to be published, in order to ensure that end-users have access to comprehensive, comparable and user-friendly information. Where appropriate, the parameters, definitions and measurement methods given in Annex III could be used.

Article 23
Integrity of the network

Member States shall take all necessary steps to ensure the integrity of the public telephone network at fixed locations and, in the event of catastrophic network breakdown or in cases of force majeure, the availability of the public telephone network and publicly available telephone services at fixed locations. Member States shall ensure that undertakings providing publicly available telephone services at fixed locations take all reasonable steps to ensure uninterrupted access to emergency services.

Article 24
Interoperability of consumer digital television equipment

In accordance with the provisions of Annex VI, Member States shall ensure the interoperability of the consumer digital television equipment referred to therein.

Article 25
Operator assistance and directory enquiry services

1. Member States shall ensure that subscribers to publicly available telephone services have the right to have an entry in the publicly available directory referred to in Article 5(1)(a).

2. Member States shall ensure that all undertakings which assign telephone numbers to subscribers meet all reasonable requests to make available, for the purposes of the provision of publicly available directory enquiry services and directories, the relevant information in an agreed format on terms which are fair, objective, cost oriented and non-discriminatory.

3. Member States shall ensure that all end-users provided with a connection to the public telephone network can access operator assistance services and directory enquiry services in accordance with Article 5(1)(b).

4. Member States shall not maintain any regulatory restrictions which prevent end-users in one Member State from accessing directly the directory enquiry service in another Member State.

5. Paragraphs 1, 2, 3 and 4 apply subject to the requirements of Community legislation on the protection of personal data and privacy and, in particular, Article 11 of Directive 97/66/EC.

Article 26
Single European emergency call number

1. Member States shall ensure that, in addition to any other national emergency call numbers specified by the national regulatory authorities, all end-users of publicly available telephone services, including users of public pay telephones, are able to call the emergency services free of charge, by using the single European emergency call number "112".

2. Member States shall ensure that calls to the single European emergency call number "112" are appropriately answered and handled in a manner best suited to the national organisation of emergency systems and within the technological possibilities of the networks.

3. Member States shall ensure that undertakings which operate public telephone networks make caller location information available to authorities handling emergencies, to the extent technically feasible, for all calls to the single European emergency call number "112".

4. Member States shall ensure that citizens are adequately informed about the existence and use of the single European emergency call number "112".

Article 27
European telephone access codes

1. Member States shall ensure that the "00" code is the standard international access code. Special arrangements for making calls between adjacent locations across borders between Member States may be established or continued. The end-users of publicly available telephone services in the locations concerned shall be fully informed of such arrangements.

2. Member States shall ensure that all undertakings that operate public telephone networks handle all calls to the European telephony numbering space, without prejudice to the need for an undertaking that operates a public telephone network to recover the cost of the conveyance of calls on its network.

Article 28
Non-geographic numbers

Member States shall ensure that end-users from other Member States are able to access non-geographic numbers within their territory where technically and economically feasible, except where a called subscriber has chosen for commercial reasons to limit access by calling parties located in specific geographical areas.

Article 29
Provision of additional facilities

1. Member States shall ensure that national regulatory authorities are able to require all undertakings that operate public telephone networks to make available to end-users the facilities listed in Annex I, Part B, subject to technical feasibility and economic viability.

2. A Member State may decide to waive paragraph 1 in all or part of its territory if it considers, after taking into account the views of interested parties, that there is sufficient access to these facilities.

3. Without prejudice to Article 10(2), Member States may impose the obligations in Annex I, Part A, point (e), concerning disconnection as a general requirement on all undertakings.

Article 30
Number portability

1. Member States shall ensure that all subscribers of publicly available telephone services, including mobile services, who so request can retain their number(s) independently of the undertaking providing the service:

   (a) in the case of geographic numbers, at a specific location; and

   (b) in the case of non-geographic numbers, at any location.

   This paragraph does not apply to the porting of numbers between networks providing services at a fixed location and mobile networks.

2. National regulatory authorities shall ensure that pricing for interconnection related to the provision of number portability is cost oriented and that direct charges to subscribers, if any, do not act as a disincentive for the use of these facilities.

3. National regulatory authorities shall not impose retail tariffs for the porting of numbers in a manner that would distort competition, such as by setting specific or common retail tariffs.

Article 31
"Must carry" obligations

1. Member States may impose reasonable "must carry" obligations, for the transmission of speci-

fied radio and television broadcast channels and services, on undertakings under their jurisdiction providing electronic communications networks used for the distribution of radio or television broadcasts to the public where a significant number of end-users of such networks use them as their principal means to receive radio and television broadcasts. Such obligations shall only be imposed where they are necessary to meet clearly defined general interest objectives and shall be proportionate and transparent. The obligations shall be subject to periodical review.

2. Neither paragraph 1 of this Article nor Article 3(2) of Directive 2002/19/EC (Access Directive) shall prejudice the ability of Member States to determine appropriate remuneration, if any, in respect of measures taken in accordance with this Article while ensuring that, in similar circumstances, there is no discrimination in the treatment of undertakings providing electronic communications networks. Where remuneration is provided for, Member States shall ensure that it is applied in a proportionate and transparent manner.

CHAPTER V
GENERAL AND FINAL PROVISIONS

Article 32
Additional mandatory services

Member States may decide to make additional services, apart from services within the universal service obligations as defined in Chapter II, publicly available in its own territory but, in such circumstances, no compensation mechanism involving specific undertakings may be imposed.

Article 33
Consultation with interested parties

1. Member States shall ensure as far as appropriate that national regulatory authorities take account of the views of end-users, and consumers (including, in particular, disabled users), manufacturers, undertakings that provide electronic communications networks and/or services on issues related to all end-user and consumer rights concerning publicly available electronic communications services, in particular where they have a significant impact on the market.

2. Where appropriate, interested parties may develop, with the guidance of national regulatory authorities, mechanisms, involving consumers, user groups and service providers, to improve the general quality of service provision by, inter alia, developing and monitoring codes of conduct and operating standards.

Article 34
Out-of-court dispute resolution

1. Member States shall ensure that transparent, simple and inexpensive out-of-court procedures are available for dealing with unresolved disputes, involving consumers, relating to issues covered by this Directive. Member States shall adopt measures to ensure that such procedures enable disputes to be settled fairly and promptly and may, where warranted, adopt a system of reimbursement and/or compensation. Member States may extend these obligations to cover disputes involving other end-users.

2. Member States shall ensure that their legislation does not hamper the establishment of complaints offices and the provision of on-line services at the appropriate territorial level to facilitate access to dispute resolution by consumers and end-users.

3. Where such disputes involve parties in different Member States, Member States shall coordinate their efforts with a view to bringing about a resolution of the dispute.

4. This Article is without prejudice to national court procedures.

Article 35
Technical adjustment

Amendments necessary to adapt Annexes I, II, III, VI and VII to technological developments or to changes in market demand shall be adopted by the Commission, acting in accordance with the procedure referred to in Article 37(2).

Article 36
Notification, monitoring and review procedures

1. National regulatory authorities shall notify to the Commission by at the latest the date of application referred to in Article 38(1), second subparagraph, and immediately in the event of any change thereafter in the names of undertakings designated as having universal service obligations under Article 8(1).

   The Commission shall make the information

available in a readily accessible form, and shall distribute it to the Communications Committee referred to in Article 37.

2. National regulatory authorities shall notify to the Commission the names of operators deemed to have significant market power for the purposes of this Directive, and the obligations imposed upon them under this Directive. Any changes affecting the obligations imposed upon undertakings or of the undertakings affected under the provisions of this Directive shall be notified to the Commission without delay.

3. The Commission shall periodically review the functioning of this Directive and report to the European Parliament and to the Council, on the first occasion not later than three years after the date of application referred to in Article 38(1), second subparagraph. The Member States and national regulatory authorities shall supply the necessary information to the Commission for this purpose.

Article 37
Committee

1. The Commission shall be assisted by the Communications Committee, set up by Article 22 of Directive 2002/21/EC (Framework Directive).

2. Where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

   The period laid down in Article 5(6) of Decision 1999/468/EC shall be three months.

3. The Committee shall adopt its rules of procedure.

Article 38
Transposition

1. Member States shall adopt and publish the laws, regulations and administrative provisions necessary to comply with this Directive by 24 July 2003 at the latest. They shall forthwith inform the Commission thereof.

   They shall apply those measures from 25 July 2003.

2. When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such a reference shall be laid down by the Member States.

3. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive and of any subsequent modifications to those provisions.

Article 39
Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 40
Addressees

This Directive is addressed to the Member States.

Done at Brussels, 7 March 2002.
For the European Parliament
The President P. Cox
For the Council
The President J. C. Aparicio

[1] OJ C 365 E, 19.12.2000, p. 238 and OJ C 332 E, 27.11.2001, p. 292.

[2] OJ C 139, 11.5.2001, p. 15.

[3] OJ C 144, 16.5.2001, p. 60.

[4] Opinion of the European Parliament of 13 June 2001 (not yet published in the Official Journal), Council Common Position of 17 September 2001 (OJ C 337, 30.11.2001, p. 55) and Decision of the European Parliament of 12 December 2001 (not yet published in the Official Journal). Council Decision of 14 February 2002.

[5] OJ L 24, 30.1.1998, p. 1.

[6] OJ L 165, 19.6.1992, p. 27. Directive as last amended by Commission Decision No 98/80/EC (OJ L 14, 20.1.1998, p. 27).

[7] See page 33 of this Official Journal.

[8] OJ L 95, 21.4.1993, p. 29.

[9] OJ L 144, 4.6.1997, p. 19.

[10] See page 7 of this Official Journal.

[11] OJ L 115, 17.4.1998, p. 31.

[12] OJ L 184, 17.7.1999, p. 23.

[13] See page 21 of this Official Journal.

[14] OJ L 101, 1.4.1998, p. 24.

[15] OJ L 199, 26.7.1997, p. 32. Directive as amended by Directive 98/61/EC (OJ L 268, 3.10.1998, p. 37).

ANNEX I

DESCRIPTION OF FACILITIES AND SERVICES REFERRED TO IN ARTICLE 10 (CONTROL OF EXPENDITURE) AND ARTICLE 29 (ADDITIONAL FACILITIES)

Part A: Facilities and services referred to in Article 10

(a) Itemised billing

Member States are to ensure that national regulatory authorities, subject to the requirements of relevant legislation on the protection of personal data and privacy, may lay down the basic level of itemised bills which are to be provided by designated undertakings (as established in Article 8) to consumers free of charge in order that they can:

(i) allow verification and control of the charges incurred in using the public telephone network at a fixed location and/or related publicly available telephone services, and

(ii) adequately monitor their usage and expenditure and thereby exercise a reasonable degree of control over their bills.

Where appropriate, additional levels of detail may be offered to subscribers at reasonable tariffs or at no charge.

Calls which are free of charge to the calling subscriber, including calls to helplines, are not to be identified in the calling subscriber's itemised bill.

(b) Selective call barring for outgoing calls, free of charge

I.e. the facility whereby the subscriber can, on request to the telephone service provider, bar outgoing calls of defined types or to defined types of numbers free of charge.

(c) Pre-payment systems

Member States are to ensure that national regulatory authorities may require designated undertakings to provide means for consumers to pay for access to the public telephone network and use of publicly available telephone services on pre-paid terms.

(d) Phased payment of connection fees

Member States are to ensure that national regulatory authorities may require designated undertakings to allow consumers to pay for connection to the public telephone network on the basis of payments phased over time.

(e) Non-payment of bills

Member States are to authorise specified measures, which are to be proportionate, non-discriminatory and published, to cover non-payment of telephone bills for use of the public telephone network at fixed locations. These measures are to ensure that due warning of any consequent service interruption or disconnection is given to the subscriber beforehand. Except in cases of fraud, persistent late payment or non-payment, these measures are to ensure, as far as is technically feasible, that any service interruption is confined to the service concerned. Disconnection for non-payment of bills should take place only after due warning is given to the subscriber. Member States may allow a period of limited service prior to complete disconnection, during which only calls that do not incur a charge to the subscriber (e.g. "112" calls) are permitted.

Part B: List of facilities referred to in Article 29

(a) Tone dialling or DTMF (dual-tone multi-frequency operation)

I.e. the public telephone network supports the use of DTMF tones as defined in ETSI ETR 207 for end-to-end signalling throughout the network both within a Member State and between Member States.

(b) Calling-line identification

I.e. the calling party's number is presented to the called party prior to the call being established.

This facility should be provided in accordance with relevant legislation on protection of personal data and privacy, in particular Directive 97/66/EC.

To the extent technically feasible, operators should provide data and signals to facilitate the offering of calling-line identity and tone dialling across Member State boundaries.

ANNEX II

INFORMATION TO BE PUBLISHED IN ACCORDANCE WITH ARTICLE 21 (TRANSPARENCY AND PUBLICATION OF INFORMATION)

The national regulatory authority has a responsibil-

Parameter[1]	Definition	Measurement method
Supply time for initial connection	ETSI EG 201 769-1	ETSI EG 201 769-1
Fault rate per access time	ETSI EG 201 769-1	ETSI EG 201 769-1
Fault repair time	ETSI EG 201 769-1	ETSI EG 201 769-1
Unsuccessful call ratio[2]	ETSI EG 201 769-1	ETSI EG 201 769-1
Call set up time[2]	ETSI EG 201 769-1	ETSI EG 201 769-1
Response times for operator services	ETSI EG 201 769-1	ETSI EG 201 769-1
Response times for directory enquiry services	ETSI EG 201 769-1	ETSI EG 201 769-1
Proportion of coin and card operated public pay telephones in workingorder	ETSI EG 201 769-1	ETSI EG 201 769-1
Bill correctness complaints	ETSI EG 201 769-1	ETSI EG 201 769-1

[1] Parameters should allow for perfomance to be analysed at a regional level (i.e. no less than Level 2 in the Nomenclature of Territorial Units for Statistics (NUTS) established by Eurostat).
[2] Member States may decide not to require that up-to-date information concerning the perfomance for these two parameters be kept, if evidence is available to show that perfomance in these two areas is satisfactory.

Note: Version number of ETSI EG 201 769-1 is 1.1.1 (April 2000)

ity to ensure that the information in this Annex is published, in accordance with Article 21. It is for the national regulatory authority to decide which information is to be published by the undertakings providing public telephone networks and/or publicly available telephone services and which information is to be published by the national regulatory authority itself, so as to ensure that consumers are able to make informed choices.

1. Name(s) and address(es) of undertaking(s)

I.e. names and head office addresses of undertakings providing public telephone networks and/or publicly available telephone services.

2. Publicly available telephone services offered

2.1 Scope of the publicly available telephone service

Description of the publicly available telephone services offered, indicating what is included in the subscription charge and the periodic rental charge (e.g. operator services, directories, directory enquiry services, selective call barring, itemised billing, maintenance, etc.).

2.2 Standard tariffs covering access, all types of usage charges, maintenance, and including details of standard discounts applied and special and targeted tariff schemes.

2.3 Compensation/refund policy, including specific details of any compensation/refund schemes offered.

2.4 Types of maintenance service offered.

2.5 Standard contract conditions, including any minimum contractual period, if relevant.

3. Dispute settlement mechanisms including those developed by the undertaking.

4. Information about rights as regards universal service, including the facilities and services mentioned in Annex I.

ANNEX III

QUALITY OF SERVICE PARAMETERS

Supply-time and quality-of-service parameters, definitions and measurement methods referred to Articles 11 and 22

ANNEX IV

CALCULATING THE NET COST, IF ANY, OF UNIVERSAL SERVICE OBLIGATIONS AND ESTABLISHING ANY RECOVERY OR SHARING MECHANISM IN ACCORDANCE WITH ARTICLES 12 AND 13

Part A: Calculation of net cost

Universal service obligations refer to those obligations placed upon an undertaking by a Member State which concern the provision of a network and service throughout a specified geographical area, including, where required, averaged prices in that geographical area for the provision of that service or provision of specific tariff options for consumers with low incomes or with special social needs.

National regulatory authorities are to consider all means to ensure appropriate incentives for undertakings (designated or not) to provide universal service obligations cost efficiently. In undertaking a calculation exercise, the net cost of universal service obligations is to be calculated as the difference between the net cost for a designated undertaking of operating with the universal service obligations and operating without the universal service obligations. This applies whether the network in a particular Member State is fully developed or is still undergoing development and expansion. Due attention is to be given to correctly assessing the costs that any designated undertaking would have chosen to avoid had there been no universal service obligation. The net cost calculation should assess the benefits, including intangible benefits, to the universal service operator.

The calculation is to be based upon the costs attributable to:

(i) elements of the identified services which can only be provided at a loss or provided under cost conditions falling outside normal commercial standards.

This category may include service elements such as access to emergency telephone services, provision of certain public pay telephones, provision of certain services or equipment for disabled people, etc;

(ii) specific end-users or groups of end-users who, taking into account the cost of providing the specified network and service, the revenue generated and any geographical averaging of prices imposed by the Member State, can only be served at a loss or under cost conditions falling outside normal commercial standards.

This category includes those end-users or groups of end-users which would not be served by a commercial operator which did not have an obligation to provide universal service.

The calculation of the net cost of specific aspects of universal service obligations is to be made separately and so as to avoid the double counting of any direct or indirect benefits and costs. The overall net cost of universal service obligations to any undertaking is to be calculated as the sum of the net costs arising from the specific components of universal service obligations, taking account of any intangible benefits. The responsibility for verifying the net cost lies with the national regulatory authority.

Part B: Recovery of any net costs of universal service obligations

The recovery or financing of any net costs of universal service obligations requires designated undertakings with universal service obligations to be compensated for the services they provide under non-commercial conditions. Because such a compensation involves financial transfers, Member States are to ensure that these are undertaken in an objective, transparent, non-discriminatory and proportionate manner. This means that the transfers result in the least distortion to competition and to user demand.

In accordance with Article 13(3), a sharing mechanism based on a fund should use a transparent and neutral means for collecting contributions that avoids the danger of a double imposition of contributions falling on both outputs and inputs of undertakings.

The independent body administering the fund is to be responsible for collecting contributions from undertakings which are assessed as liable to contribute to the net cost of universal service obligations in the Member State and is to oversee the transfer of sums due and/or administrative payments to the undertakings entitled to receive payments from the fund.

ANNEX V

PROCESS FOR REVIEWING THE SCOPE OF UNIVERSAL SERVICE IN ACCORDANCE WITH ARTICLE 15

In considering whether a review of the scope of universal service obligations should be undertaken, the Commission is to take into consideration the following elements:

- social and market developments in terms of the services used by consumers,
- social and market developments in terms of

the availability and choice of services to consumers,

- technological developments in terms of the way services are provided to consumers.

In considering whether the scope of universal service obligations be changed or redefined, the Commission is to take into consideration the following elements:

- are specific services available to and used by a majority of consumers and does the lack of availability or non-use by a minority of consumers result in social exclusion, and
- does the availability and use of specific services convey a general net benefit to all consumers such that public intervention is warranted in circumstances where the specific services are not provided to the public under normal commercial circumstances?

ANNEX VI

INTEROPERABILITY OF DIGITAL CONSUMER EQUIPMENT REFERRED TO IN ARTICLE 24

1. The common scrambling algorithm and free-to-air reception

   All consumer equipment intended for the reception of digital television signals, for sale or rent or otherwise made available in the Community, capable of descrambling digital television signals, is to possess the capability to:

   - allow the descrambling of such signals according to the common European scrambling algorithm as administered by a recognised European standards organisation, currently ETSI;
   - display signals that have been transmitted in clear provided that, in the event that such equipment is rented, the rentee is in compliance with the relevant rental agreement.

2. Interoperability for analogue and digital television sets

   Any analogue television set with an integral screen of visible diagonal greater than 42 cm which is put on the market for sale or rent in the Community is to be fitted with at least one open interface socket, as standardised by a recognised European standards organisation, e.g. as given in the CENELEC EN 50 049-1:1997 standard, permitting simple connection of peripherals, especially additional decoders and digital receivers.

   Any digital television set with an integral screen of visible diagonal greater than 30 cm which is put on the market for sale or rent in the Community is to be fitted with at least one open interface socket (either standardised by, or conforming to a standard adopted by, a recognised European standards organisation, or conforming to an industry-wide specification) e.g. the DVB common interface connector, permitting simple connection of peripherals, and able to pass all the elements of a digital television signal, including information relating to interactive and conditionally accessed services.

ANNEX VII

CONDITIONS FOR THE MINIMUM SET OF LEASED LINES REFERRED TO IN ARTICLE 18

Note:

In accordance with the procedure in Article 18, provision of the minimum set of leased lines under the conditions established by Directive 92/44/EC should continue until such time as the national regulatory authority determines that there is effective competition in the relevant leased lines market.

National regulatory authorities are to ensure that provision of the minimum set of leased lines referred to in Article 18 follows the basic principles of non-discrimination, cost orientation and transparency.

1. Non discrimination

   National regulatory authorities are to ensure that the organisations identified as having significant market power pursuant to Article 18(1) adhere to the principle of non-discrimination when providing leased lines referred to in Article 18. Those organisations are to apply similar conditions in similar circumstances to organisations providing similar services, and are to provide leased lines to others under the same conditions and of the same quality as they provide for their own services, or those of their subsidiaries or partners, where applicable.

2. Cost orientation

   National regulatory authorities are, where appropriate, to ensure that tariffs for leased lines referred to in Article 18 follow the basic princi-

ples of cost orientation.

To this end, national regulatory authorities are to ensure that undertakings identified as having significant market power pursuant to Article 18(1) formulate and put in practice a suitable cost accounting system.

National regulatory authorities are to keep available, with an adequate level of detail, information on the cost accounting systems applied by such undertakings. They are to submit this information to the Commission on request.

3. Transparency

National regulatory authorities are to ensure that the following information in respect of the minimum set of leased lines referred to in Article 18 is published in an easily accessible form.

3.1 Technical characteristics, including the physical and electrical characteristics as well as the detailed technical and performance specifications which apply at the network termination point.

3.2 Tariffs, including the initial connection charges, the periodic rental charges and other charges. Where tariffs are differentiated, this must be indicated.

Where, in response to a particular request, an organisation identified as having significant market power pursuant to Article 18(1) considers it unreasonable to provide a leased line in the minimum set under its published tariffs and supply conditions, it must seek the agreement of the national regulatory authority to vary those conditions in that case.

3.3 Supply conditions, including at least the following elements:

- information concerning the ordering procedure,
- the typical delivery period, which is the period, counted from the date when the user has made a firm request for a leased line, in which 95 % of all leased lines of the same type have been put through to the customers.

This period will be established on the basis of the actual delivery periods of leased lines during a recent time interval of reasonable duration. The calculation must not include cases where late delivery periods were requested by users,

- the contractual period, which includes the period which is in general laid down in the contract and the minimum contractual period which the user is obliged to accept,
- the typical repair time, which is the period, counted from the time when a failure message has been given to the responsible unit within the undertaking identified as having significant market power pursuant to Article 18(1) up to the moment in which 80 % of all leased lines of the same type have been re-established and in appropriate cases notified back in operation to the users. Where different classes of quality of repair are offered for the same type of leased lines, the different typical repair times shall be published,
- any refund procedure.

In addition where a Member State considers that the achieved performance for the provision of the minimum set of leased lines does not meet users' needs, it may define appropriate targets for the supply conditions listed above.

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)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission(1),

Having regard to the opinion of the Economic and Social Committee(2),

Having consulted the Committee of the Regions,

Acting in accordance with the procedure laid down in Article 251 of the Treaty(3),

Whereas:

(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data(4) requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.

(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

(3) Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States.

(4) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(5) translated the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector. Directive 97/66/EC has to be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used. That Directive should therefore be repealed and replaced by this Directive.

(5) New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the information society is characterised by the introduction of new electronic communications services. Access to digital mobile networks has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.

(6) The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.

(7) In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.

(8) Legal, regulatory and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interest of legal persons, in the

electronic communication sector, should be harmonised in order to avoid obstacles to the internal market for electronic communication in accordance with Article 14 of the Treaty. Harmonisation should be limited to requirements necessary to guarantee that the promotion and development of new electronic communications services and networks between Member States are not hindered.

(9) The Member States, providers and users concerned, together with the competent Community bodies, should cooperate in introducing and developing the relevant technologies where this is necessary to apply the guarantees provided for by this Directive and taking particular account of the objectives of minimising the processing of personal data and of using anonymous or pseudonymous data where possible.

(10) In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services.

(11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(12) Subscribers to a publicly available electronic communications service may be natural or legal persons. By supplementing Directive 95/46/EC, this Directive is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons. This Directive does not entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons, which is ensured within the framework of the applicable Community and national legislation.

(13) The contractual relation between a subscriber and a service provider may entail a periodic or a one-off payment for the service provided or to be provided. Prepaid cards are also considered as a contract.

(14) Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

(15) A communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication. Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. Traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.

(16) Information that is part of a broadcasting service provided over a public communications network is intended for a potentially unlimited audience and does not constitute a communication in the sense of this Directive. However, in cases where the individual subscriber or user receiving such information can be identified, for example with video-on-demand services, the information conveyed is covered within the meaning of a communication for the purposes of this Directive.

(17) For the purposes of this Directive, consent of a

user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website.

(18) Value added services may, for example, consist of advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information.

(19) The application of certain requirements relating to presentation and restriction of calling and connected line identification and to automatic call forwarding to subscriber lines connected to analogue exchanges should not be made mandatory in specific cases where such application would prove to be technically impossible or would require a disproportionate economic effort. It is important for interested parties to be informed of such cases and the Member States should therefore notify them to the Commission.

(20) Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet or analogue mobile telephony. It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing security risks which lie outside the scope of possible remedies by the service provider. Service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge except for any nominal costs which the subscriber may incur while receiving or collecting the information, for instance by downloading an electronic mail message. Security is appraised in the light of Article 17 of Directive 95/46/EC.

(21) Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.

(22) The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. Where this is necessary for making more efficient the onward transmission of any publicly accessible information to other recipients of the service upon their request, this Directive should not prevent such information from being further stored, provided that this information would in any case be accessible to the public without restriction and that any data referring to the individual subscribers or users requesting such information are erased.

(23) Confidentiality of communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction. Directive 95/46/EC applies to such processing. Parties to the communications should be informed prior to the recording about the recording, its purpose and the duration of its storage. The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged.

(24) Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the

Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.

(25) However, such devices, for instance so-called "cookies", can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

(26) The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data which the provider of the publicly available electronic communications services may want to perform, for the marketing of electronic communications services or for the provision of value added services, may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing. Traffic data used for marketing communications services or for the provision of value added services should also be erased or made anonymous after the provision of the service. Service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done.

(27) The exact moment of the completion of the transmission of a communication, after which traffic data should be erased except for billing purposes, may depend on the type of electronic communications service that is provided. For instance for a voice telephony call the transmission will be completed as soon as either of the users terminates the connection. For electronic mail the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider.

(28) The obligation to erase traffic data or to make such data anonymous when it is no longer needed for the purpose of the transmission of a communication does not conflict with such procedures on the Internet as the caching in the domain name system of IP addresses or the caching of IP addresses to physical address bindings or the use of log-in information to control the right of access to networks or services.

(29) The service provider may process traffic data relating to subscribers and users where necessary in individual cases in order to detect technical failure or errors in the transmission of communications. Traffic data necessary for billing purposes may also be processed by the provider in order to detect and stop fraud consisting of unpaid use of the electronic communications service.

(30) Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing

thereof should be based on aggregated, traffic data that cannot be related to subscribers or users. Where such activities cannot be based on aggregated data, they should be considered as value added services for which the consent of the subscriber is required.

(31) Whether the consent to be obtained for the processing of personal data with a view to providing a particular value added service should be that of the user or of the subscriber, will depend on the data to be processed and on the type of service to be provided and on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it.

(32) Where the provider of an electronic communications service or of a value added service subcontracts the processing of personal data necessary for the provision of these services to another entity, such subcontracting and subsequent data processing should be in full compliance with the requirements regarding controllers and processors of personal data as set out in Directive 95/46/EC. Where the provision of a value added service requires that traffic or location data are forwarded from an electronic communications service provider to a provider of value added services, the subscribers or users to whom the data are related should also be fully informed of this forwarding before giving their consent for the processing of the data.

(33) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services, for example calling cards and facilities for payment by credit card. To the same end, Member States may ask the operators to offer their subscribers a different type of detailed bill in which a certain number of digits of the called number have been deleted.

(34) It is necessary, as regards calling line identification, to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. There is justification for overriding the elimination of calling line identification presentation in specific cases. Certain subscribers, in particular help lines and similar organisations, have an interest in guaranteeing the anonymity of their callers. It is necessary, as regards connected line identification, to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected, in particular in the case of forwarded calls. The providers of publicly available electronic communications services should inform their subscribers of the existence of calling and connected line identification in the network and of all services which are offered on the basis of calling and connected line identification as well as the privacy options which are available. This will allow the subscribers to make an informed choice about the privacy facilities they may want to use. The privacy options which are offered on a per-line basis do not necessarily have to be available as an automatic network service but may be obtainable through a simple request to the provider of the publicly available electronic communications service.

(35) In digital mobile networks, location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications. Such data are traffic data covered by Article 6 of this Directive. However, in addition, digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualised traffic information and guidance to drivers. The processing of such data for value added services should only be allowed where subscribers have given their consent. Even in cases where subscribers have given their consent, they should have a simple means to temporarily deny the processing of location data, free of charge.

(36) Member States may restrict the users' and subscribers' rights to privacy with regard to calling line identification where this is necessary to trace nuisance calls and with regard to calling line identification and location data where this is necessary to allow emergency services to carry out their tasks as effectively as possible. For these purposes, Member States may adopt specific provisions to entitle providers of elec-

tronic communications services to provide access to calling line identification and location data without the prior consent of the users or subscribers concerned.

(37) Safeguards should be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others. Moreover, in such cases, it must be possible for subscribers to stop the forwarded calls being passed on to their terminals by simple request to the provider of the publicly available electronic communications service.

(38) Directories of subscribers to electronic communications services are widely distributed and public. The right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine whether their personal data are published in a directory and if so, which. Providers of public directories should inform the subscribers to be included in such directories of the purposes of the directory and of any particular usage which may be made of electronic versions of public directories especially through search functions embedded in the software, such as reverse search functions enabling users of the directory to discover the name and address of the subscriber on the basis of a telephone number only.

(39) The obligation to inform subscribers of the purpose(s) of public directories in which their personal data are to be included should be imposed on the party collecting the data for such inclusion. Where the data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients. Any transmission should be subject to the condition that the data may not be used for other purposes than those for which they were collected. If the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted.

(40) Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a harmonised approach to ensure simple, Community-wide rules for businesses and users.

(41) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/EC. When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.

(42) Other forms of direct marketing that are more costly for the sender and impose no financial costs on subscribers and users, such as person-to-person voice telephony calls, may justify the maintenance of a system giving subscribers or users the possibility to indicate that they do not want to receive such calls. Nevertheless, in order not to decrease existing levels of privacy protection, Member States should be entitled to uphold national systems, only allowing such calls to subscribers and users who have given their prior consent.

(43) To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.

(44) Certain electronic mail systems allow subscribers to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments, thereby reducing costs which could arise from downloading unsolicited electronic mails or attachments. These arrangements may continue to be useful in certain cases as an additional tool to the general obligations established in

this Directive.

(45) This Directive is without prejudice to the arrangements which Member States make to protect the legitimate interests of legal persons with regard to unsolicited communications for direct marketing purposes. Where Member States establish an opt-out register for such communications to legal persons, mostly business users, the provisions of Article 7 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce)(6) are fully applicable.

(46) The functionalities for the provision of electronic communications services may be integrated in the network or in any part of the terminal equipment of the user, including the software. The protection of the personal data and the privacy of the user of publicly available electronic communications services should be independent of the configuration of the various components necessary to provide the service and of the distribution of the necessary functionalities between these components. Directive 95/46/EC covers any form of processing of personal data regardless of the technology used. The existence of specific rules for electronic communications services alongside general rules for other components necessary for the provision of such services may not facilitate the protection of personal data and privacy in a technologically neutral way. It may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected. The adoption of such measures in accordance with Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity(7) will ensure that the introduction of technical features of electronic communication equipment including software for data protection purposes is harmonised in order to be compatible with the implementation of the internal market.

(47) Where the rights of the users and subscribers are not respected, national legislation should provide for judicial remedies. Penalties should be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive.

(48) It is useful, in the field of application of this Directive, to draw on the experience of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data composed of representatives of the supervisory authorities of the Member States, set up by Article 29 of Directive 95/46/EC.

(49) To facilitate compliance with the provisions of this Directive, certain specific arrangements are needed for processing of data already under way on the date that national implementing legislation pursuant to this Directive enters into force,

HAVE ADOPTED THIS DIRECTIVE:

Article 1
Scope and aim

1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Article 2
Definitions

Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services

(Framework Directive)(8) shall apply.

The following definitions shall also apply:

(a) "user" means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;

(b) "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

(c) "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

(d) "communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

(e) "call" means a connection established by means of a publicly available telephone service allowing two-way communication in real time;

(f) "consent" by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC;

(g) "value added service" means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;

(h) "electronic mail" means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Article 3
Services concerned

1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.

2. Articles 8, 10 and 11 shall apply to subscriber lines connected to digital exchanges and, where technically possible and if it does not require a disproportionate economic effort, to subscriber lines connected to analogue exchanges.

3. Cases where it would be technically impossible or require a disproportionate economic effort to fulfil the requirements of Articles 8, 10 and 11 shall be notified to the Commission by the Member States.

Article 4
Security

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

Article 5
Confidentiality of the communications

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of

providing evidence of a commercial transaction or of any other business communication.

3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

Article 6
Traffic data

1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

Article 7
Itemised billing

1. Subscribers shall have the right to receive non-itemised bills.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative privacy enhancing methods of communications or payments are available to such users and subscribers.

Article 8
Presentation and restriction of calling and connected line identification

1. Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

2. Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls.

3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presenta-

tion of the calling line identification has been prevented by the calling user or subscriber.

4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user.

5. Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.

6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

Article 9
Location data other than traffic data

1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

Article 10
Exceptions

Member States shall ensure that there are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service may override:

(a) the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public communications network and/or publicly available electronic communications service;

(b) the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.

Article 11
Automatic call forwarding

Member States shall ensure that any subscriber has the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber's terminal.

Article 12
Directories of subscribers

1. Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.

2. Member States shall ensure that subscribers are given the opportunity to determine whether

their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.

3. Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers.

4. Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.

Article 13
Unsolicited communications

1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

Article 14
Technical features and standardisation

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs 2 and 3, that no mandatory requirements for specific technical features are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

2. Where provisions of this Directive can be implemented only by requiring specific technical features in electronic communications networks, Member States shall inform the Commission in accordance with the procedure provided for by Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services(9).

3. Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications(10).

Article 15
Application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive

when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.

3. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.

Article 16
Transitional arrangements

1. Article 12 shall not apply to editions of directories already produced or placed on the market in printed or off-line electronic form before the national provisions adopted pursuant to this Directive enter into force.

2. Where the personal data of subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with the provisions of Directive 95/46/EC and of Article 11 of Directive 97/66/EC before the national provisions adopted in pursuance of this Directive enter into force, the personal data of such subscribers may remain included in this public directory in its printed or electronic versions, including versions with reverse search functions, unless subscribers indicate otherwise, after having received complete information about purposes and options in accordance with Article 12 of this Directive.

Article 17
Transposition

1. Before 31 October 2003 Member States shall bring into force the provisions necessary to comply with this Directive. They shall forthwith inform the Commission thereof.

   When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive and of any subsequent amendments to those provisions.

Article 18
Review

The Commission shall submit to the European Parliament and the Council, not later than three years after the date referred to in Article 17(1), a report on the application of this Directive and its impact on economic operators and consumers, in particular as regards the provisions on unsolicited communications, taking into account the international environment. For this purpose, the Commission may request information from the Member States, which shall be supplied without undue delay. Where appropriate, the Commission shall submit proposals to amend this Directive, taking account of the results of that report, any changes in the sector and any other proposal it may deem necessary in order to improve the effectiveness of this Directive.

Article 19
Repeal

Directive 97/66/EC is hereby repealed with effect from the date referred to in Article 17(1).

References made to the repealed Directive shall be construed as being made to this Directive.

Article 20
Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 21
Addressees

This Directive is addressed to the Member States.

Done at Brussels, 12 July 2002.
For the European Parliament
The President P. Cox
For the Council
The President T. Pedersen

[1] OJ C 365 E, 19.12.2000, p. 223.

[2] OJ C 123, 25.4.2001, p. 53.

[3] Opinion of the European Parliament of 13 November 2001 (not yet published in the Official Journal), Council Common Position of 28 January 2002 (OJ C 113 E, 14.5.2002, p. 39) and Decision of the European Parliament of 30 May 2002 (not yet published in the Official Journal). Council Decision of 25 June 2002.

[4] OJ L 281, 23.11.1995, p. 31.

[5] OJ L 24, 30.1.1998, p. 1.

[6] OJ L 178, 17.7.2000, p. 1.

[7] OJ L 91, 7.4.1999, p. 10.

[8] OJ L 108, 24.4.2002, p. 33.

[9] OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).

[10] OJ L 36, 7.2.1987, p. 31. Decision as last amended by the 1994 Act of Accession.

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission(1),

Having regard to the opinion of the European Economic and Social Committee(2),

Having regard to the opinion of the Committee of the Regions(3),

Acting in accordance with the procedure set out in Article 251 of the Treaty(4),

Whereas:

(1) The Treaty provides for the establishment of an internal market and of a system ensuring that competition in the internal market is not distorted. Harmonisation of the rules and practices in the Member States relating to the exploitation of public sector information contributes to the achievement of these objectives.

(2) The evolution towards an information and knowledge society influences the life of every citizen in the Community, inter alia, by enabling them to gain new ways of accessing and acquiring knowledge.

(3) Digital content plays an important role in this evolution. Content production has given rise to rapid job creation in recent years and continues to do so. Most of these jobs are created in small emerging companies.

(4) The public sector collects, produces, reproduces and disseminates a wide range of information in many areas of activity, such as social, economic, geographical, weather, tourist, business, patent and educational information.

(5) One of the principal aims of the establishment

of an internal market is the creation of conditions conducive to the development of Community-wide services. Public sector information is an important primary material for digital content products and services and will become an even more important content resource with the development of wireless content services. Broad cross-border geographical coverage will also be essential in this context. Wider possibilities of re-using public sector information should inter alia allow European companies to exploit its potential and contribute to economic growth and job creation.

(6) There are considerable differences in the rules and practices in the Member States relating to the exploitation of public sector information resources, which constitute barriers to bringing out the full economic potential of this key document resource. Traditional practice in public sector bodies in exploiting public sector information has developed in very disparate ways. That should be taken into account. Minimum harmonisation of national rules and practices on the re-use of public sector documents should therefore be undertaken, in cases where the differences in national regulations and practices or the absence of clarity hinder the smooth functioning of the internal market and the proper development of the information society in the Community.

(7) Moreover, without minimum harmonisation at Community level, legislative activities at national level, which have already been initiated in a number of Member States in order to respond to the technological challenges, might result in even more significant differences. The impact of such legislative differences and uncertainties will become more significant with the further development of the information society, which has already greatly increased cross-border exploitation of information.

(8) A general framework for the conditions governing re-use of public sector documents is needed in order to ensure fair, proportionate and non-discriminatory conditions for the re-use of such information. Public sector bodies collect, produce, reproduce and disseminate documents to fulfil their public tasks. Use of such documents for other reasons constitutes a re-use. Member States' policies can go beyond the minimum standards established in this Directive, thus allowing for more extensive re-use.

(9) This Directive does not contain an obligation to allow re-use of documents. The decision whether or not to authorise re-use will remain with the Member States or the public sector body concerned. This Directive should apply to documents that are made accessible for re-use when public sector bodies license, sell, disseminate, exchange or give out information. To avoid cross-subsidies, re-use should include further use of documents within the organisation itself for activities falling outside the scope of its public tasks. Activities falling outside the public task will typically include supply of documents that are produced and charged for exclusively on a commercial basis and in competition with others in the market. The definition of "document" is not intended to cover computer programmes. The Directive builds on the existing access regimes in the Member States and does not change the national rules for access to documents. It does not apply in cases in which citizens or companies can, under the relevant access regime, only obtain a document if they can prove a particular interest. At Community level, Articles 41 (right to good administration) and 42 of the Charter of Fundamental Rights of the European Union recognise the right of any citizen of the Union and any natural or legal person residing or having its registered office in a Member State to have access to European Parliament, Council and Commission documents. Public sector bodies should be encouraged to make available for re-use any documents held by them. Public sector bodies should promote and encourage re-use of documents, including official texts of a legislative and administrative nature in those cases where the public sector body has the right to authorise their re-use.

(10) The definitions of "public sector body" and "body governed by public law" are taken from the public procurement Directives (92/50/EEC(5), 93/36/EEC(6) and 93/37/EEC(7) and 98/4/EC(8)). Public undertakings are not covered by these definitions.(11) This Directive lays down a generic definition of the term "document", in line with developments in the information society. It covers any representation of acts, facts or information - and any compilation of such acts, facts or information - whatever its medium (written on paper, or stored in electronic form or as a sound, visual or audiovisual recording), held by public sector bodies. A document held by a public sector body is a document where the public sector body has the right to authorise re-use.

(11) The time limit for replying to requests for re-use should be reasonable and in line with the equivalent time for requests to access the document

under the relevant access regimes. Reasonable time limits throughout the Union will stimulate the creation of new aggregated information products and services at pan-European level. Once a request for re-use has been granted, public sector bodies should make the documents available in a timeframe that allows their full economic potential to be exploited. This is particularly important for dynamic content (e.g. traffic data), the economic value of which depends on the immediate availability of the information and of regular updates. Should a licence be used, the timely availability of documents may be a part of the terms of the licence.

(12) The possibilities for re-use can be improved by limiting the need to digitise paper-based documents or to process digital files to make them mutually compatible. Therefore, public sector bodies should make documents available in any pre-existing format or language, through electronic means where possible and appropriate. Public sector bodies should view requests for extracts from existing documents favourably when to grant such a request would involve only a simple operation. Public sector bodies should not, however, be obliged to provide an extract from a document where this involves disproportionate effort. To facilitate re-use, public sector bodies should make their own documents available in a format which, as far as possible and appropriate, is not dependent on the use of specific software. Where possible and appropriate, public sector bodies should take into account the possibilities for the re-use of documents by and for people with disabilities.

(13) Where charges are made, the total income should not exceed the total costs of collecting, producing, reproducing and disseminating documents, together with a reasonable return on investment, having due regard to the self-financing requirements of the public sector body concerned, where applicable. Production includes creation and collation, and dissemination may also include user support. Recovery of costs, together with a reasonable return on investment, consistent with applicable accounting principles and the relevant cost calculation method of the public sector body concerned, constitutes an upper limit to the charges, as any excessive prices should be precluded. The upper limit for charges set in this Directive is without prejudice to the right of Member States or public sector bodies to apply lower charges or no charges at all, and Member States should encourage public sector bodies to make documents available at charges that do not exceed the marginal costs for reproducing and disseminating the documents.

(14) Ensuring that the conditions for re-use of public sector documents are clear and publicly available is a pre-condition for the development of a Community-wide information market. Therefore all applicable conditions for the re-use of the documents should be made clear to the potential re-users. Member States should encourage the creation of indices accessible on line, where appropriate, of available documents so as to promote and facilitate requests for re-use. Applicants for re-use of documents should be informed of available means of redress relating to decisions or practices affecting them. This will be particularly important for SMEs which may not be familiar with interactions with public sector bodies from other Member States and corresponding means of redress.

(15) Making public all generally available documents held by the public sector - concerning not only the political process but also the legal and administrative process - is a fundamental instrument for extending the right to knowledge, which is a basic principle of democracy. This objective is applicable to institutions at every level, be it local, national or international.

(16) In some cases the re-use of documents will take place without a licence being agreed. In other cases a licence will be issued imposing conditions on the re-use by the licensee dealing with issues such as liability, the proper use of documents, guaranteeing non-alteration and the acknowledgement of source. If public sector bodies license documents for re-use, the licence conditions should be fair and transparent. Standard licences that are available online may also play an important role in this respect. Therefore Member States should provide for the availability of standard licences.

(17) If the competent authority decides to no longer make available certain documents for re-use, or to cease updating these documents, it should make these decisions publicly known, at the earliest opportunity, via electronic means whenever possible.

(18) Conditions for re-use should be non-discriminatory for comparable categories of re-use. This should, for example, not prevent the exchange of information between public sector bodies free of charge for the exercise of public tasks, whilst other parties are charged for the re-use of the same documents. Neither should it prevent the adoption of a differentiated charging policy

for commercial and non-commercial re-use.

(19) Public sector bodies should respect competition rules when establishing the principles for re-use of documents avoiding as far as possible exclusive agreements between themselves and private partners. However, in order to provide a service of general economic interest, an exclusive right to re-use specific public sector documents may sometimes be necessary. This may be the case if no commercial publisher would publish the information without such an exclusive right.

(20) This Directive should be implemented and applied in full compliance with the principles relating to the protection of personal data in accordance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and of the free movement of such data(9).

(21) The intellectual property rights of third parties are not affected by this Directive. For the avoidance of doubt, the term "intellectual property rights" refers to copyright and related rights only (including sui generis forms of protection). This Directive does not apply to documents covered by industrial property rights, such as patents, registered designs and trademarks. The Directive does not affect the existence or ownership of intellectual property rights of public sector bodies, nor does it limit the exercise of these rights in any way beyond the boundaries set by this Directive. The obligations imposed by this Directive should apply only insofar as they are compatible with the provisions of international agreements on the protection of intellectual property rights, in particular the Berne Convention for the Protection of Literary and Artistic Works (the Berne Convention) and the Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS Agreement). Public sector bodies should, however, exercise their copyright in a way that facilitates re-use.

(22) Tools that help potential re-users to find documents available for re-use and the conditions for re-use can facilitate considerably the cross-border use of public sector documents. Member States should therefore ensure that practical arrangements are in place that help re-users in their search for documents available for re-use. Assets lists, accessible preferably online, of main documents (documents that are extensively re-used or that have the potential to be extensively re-used), and portal sites that are linked to decentralised assets lists are examples of such practical arrangements.

(23) This Directive is without prejudice to Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society(10) and Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases(11). It spells out the conditions within which public sector bodies can exercise their intellectual property rights in the internal information market when allowing re-use of documents.

(24) Since the objectives of the proposed action, namely to facilitate the creation of Community-wide information products and services based on public sector documents, to enhance an effective cross-border use of public sector documents by private companies for added-value information products and services and to limit distortions of competition on the Community market, cannot be sufficiently achieved by the Member States and can therefore, in view of the intrinsic Community scope and impact of the said action, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives. This Directive should achieve minimum harmonisation, thereby avoiding further disparities between the Member States in dealing with the re-use of public sector documents,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I
GENERAL PROVISIONS

Article 1
Subject matter and scope

1. This Directive establishes a minimum set of rules governing the re-use and the practical means of facilitating re-use of existing documents held by public sector bodies of the Member States.

2. This Directive shall not apply to:

   (a) documents the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned

as defined by law or by other binding rules in the Member State, or in the absence of such rules as defined in line with common administrative practice in the Member State in question;

(b) documents for which third parties hold intellectual property rights;

(c) documents which are excluded from access by virtue of the access regimes in the Member States, including on the grounds of:

- the protection of national security (i.e. State security), defence, or public security,
- statistical or commercial confidentiality;

(d) documents held by public service broadcasters and their subsidiaries, and by other bodies or their subsidiaries for the fulfilment of a public service broadcasting remit;

(e) documents held by educational and research establishments, such as schools, universities, archives, libraries and research facilities including, where relevant, organisations established for the transfer of research results;

(f) documents held by cultural establishments, such as museums, libraries, archives, orchestras, operas, ballets and theatres.

3. This Directive builds on and is without prejudice to the existing access regimes in the Member States. This Directive shall not apply in cases in which citizens or companies have to prove a particular interest under the access regime to obtain access to the documents.

4. This Directive leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data under the provisions of Community and national law, and in particular does not alter the obligations and rights set out in Directive 95/46/EC.

5. The obligations imposed by this Directive shall apply only insofar as they are compatible with the provisions of international agreements on the protection of intellectual property rights, in particular the Berne Convention and the TRIPS Agreement.

Article 2
Definitions

For the purpose of this Directive the following definitions shall apply:

1. "public sector body" means the State, regional or local authorities, bodies governed by public law and associations formed by one or several such authorities or one or several such bodies governed by public law;

2. "body governed by public law" means any body:

(a) established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character; and

(b) having legal personality; and

(c) financed, for the most part by the State, or regional or local authorities, or other bodies governed by public law; or subject to management supervision by those bodies; or having an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities or by other bodies governed by public law;

3. "document" means:

(a) any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording);

(b) any part of such content;

4. "re-use" means the use by persons or legal entities of documents held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced. Exchange of documents between public sector bodies purely in pursuit of their public tasks does not constitute re-use;

5. "personal data" means data as defined in Article 2(a) of Directive 95/46/EC.

Article 3
General principle

Member States shall ensure that, where the re-use of documents held by public sector bodies is allowed, these documents shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV. Where possible, documents shall be made available through electronic means.

CHAPTER II
REQUESTS FOR RE-USE

Article 4
Requirements applicable to the processing of requests for re-use

1. Public sector bodies shall, through electronic means where possible and appropriate, process requests for re-use and shall make the document available for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant within a reasonable time that is consistent with the time-frames laid down for the processing of requests for access to documents.

2. Where no time limits or other rules regulating the timely provision of documents have been established, public sector bodies shall process the request and shall deliver the documents for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant within a timeframe of not more than 20 working days after its receipt. This timeframe may be extended by another 20 working days for extensive or complex requests. In such cases the applicant shall be notified within three weeks after the initial request that more time is needed to process it.

3. In the event of a negative decision, the public sector bodies shall communicate the grounds for refusal to the applicant on the basis of the relevant provisions of the access regime in that Member State or of the national provisions adopted pursuant to this Directive, in particular Article 1(2)(a), (b) and (c), or Article 3. Where a negative decision is based on Article 1(2)(b), the public sector body shall include a reference to the natural or legal person who is the right-holder, where known, or alternatively to the licensor from which the public sector body has obtained the relevant material.

4. Any negative decision shall contain a reference to the means of redress in case the applicant wishes to appeal the decision.

5. Public sector bodies covered under Article 1(2) (d), (e) and (f) shall not be required to comply with the requirements of this Article.

CHAPTER III
CONDITIONS FOR RE-USE

Article 5
Available formats

1. Public sector bodies shall make their documents available in any pre-existing format or language, through electronic means where possible and appropriate. This shall not imply an obligation for public sector bodies to create or adapt documents in order to comply with the request, nor shall it imply an obligation to provide extracts from documents where this would involve disproportionate effort, going beyond a simple operation.

2. On the basis of this Directive, public sector bodies cannot be required to continue the production of a certain type of documents with a view to the re-use of such documents by a private or public sector organisation.

Article 6
Principles governing charging

Where charges are made, the total income from supplying and allowing re-use of documents shall not exceed the cost of collection, production, reproduction and dissemination, together with a reasonable return on investment. Charges should be cost-oriented over the appropriate accounting period and calculated in line with the accounting principles applicable to the public sector bodies involved.

Article 7
Transparency

Any applicable conditions and standard charges for the re-use of documents held by public sector bodies shall be pre-established and published, through electronic means where possible and appropriate. On request, the public sector body shall indicate the calculation basis for the published charge. The public sector body in question shall also indicate which factors will be taken into account in the calculation of charges for atypical cases. Public sector bodies shall ensure that applicants for re-use of documents are informed of available means of redress relating to decisions or practices affecting them.

Article 8
Licences

1. Public sector bodies may allow for re-use of documents without conditions or may im-

pose conditions, where appropriate through a licence, dealing with relevant issues. These conditions shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition.

2. In Member States where licences are used, Member States shall ensure that standard licences for the re-use of public sector documents, which can be adapted to meet particular licence applications, are available in digital format and can be processed electronically. Member States shall encourage all public sector bodies to use the standard licences.

Article 9
Practical arrangements

Member States shall ensure that practical arrangements are in place that facilitate the search for documents available for re-use, such as assets lists, accessible preferably online, of main documents, and portal sites that are linked to decentralised assets lists.

CHAPTER IV
NON-DISCRIMINATION AND FAIR TRADING

Article 10
Non-discrimination

1. Any applicable conditions for the re-use of documents shall be non-discriminatory for comparable categories of re-use.

2. If documents are re-used by a public sector body as input for its commercial activities which fall outside the scope of its public tasks, the same charges and other conditions shall apply to the supply of the documents for those activities as apply to other users.

Article 11
Prohibition of exclusive arrangements

1. The re-use of documents shall be open to all potential actors in the market, even if one or more market players already exploit added-value products based on these documents. Contracts or other arrangements between the public sector bodies holding the documents and third parties shall not grant exclusive rights.

2. However, where an exclusive right is necessary for the provision of a service in the public interest, the validity of the reason for granting such an exclusive right shall be subject to regular review, and shall, in any event, be reviewed every three years. The exclusive arrangements established after the entry into force of this Directive shall be transparent and made public.

3. Existing exclusive arrangements that do not qualify for the exception under paragraph 2 shall be terminated at the end of the contract or in any case not later than 31 December 2008.

CHAPTER V
FINAL PROVISIONS

Article 12
Implementation

Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 1 July 2005. They shall forthwith inform the Commission thereof.

When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

Article 13
Review

1. The Commission shall carry out a review of the application of this Directive before 1 July 2008 and shall communicate the results of this review, together with any proposals for modifications of the Directive, to the European Parliament and the Council.

2. The review shall in particular address the scope and impact of this Directive, including the extent of the increase in re-use of public sector documents, the effects of the principles applied to charging and the re-use of official texts of a legislative and administrative nature, as well as further possibilities of improving the proper functioning of the internal market and the development of the European content industry.

Article 14
Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Union.

Article 15
Addressees

This Directive is addressed to the Member States.

Done at Brussels, 17 November 2003.
For the Parliament
The President P. Cox
For the Council
The President G. Alemanno

[1] OJ C 227 E, 24.9.2002, p. 382.

[2] OJ C 85, 8.4.2003, p. 25.

[3] OJ C 73, 26.3.2003, p. 38.

[4] Opinion of the European Parliament of 12 February 2003 (not yet published in the Official Journal), Council Common Position of 26 May 2003 (OJ C 159 E, 8.7.2003, p. 1) and Position of the European Parliament of 25 September 2003 (not yet published in the Official Journal). Council Decision of 27 October 2003.

[5] OJ L 209, 24.7.1992, p. 1. Directive as last amended by Commission Directive 2001/78/EC (OJ L 285, 29.10.2001, p. 1).

[6] OJ L 199, 9.8.1993, p. 1. Directive as last amended by Commission Directive 2001/78/EC.

[7] OJ L 199, 9.8.1993, p. 54. Directive as last amended by Commission Directive 2001/78/EC.

[8] OJ L 101, 1.4.1998, p. 1.

[9] OJ L 281, 23.11.1995, p. 31.

[10] OJ L 167, 22.6.2001, p. 10.

[11] OJ L 77, 27.3.1996, p. 20.

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'

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[96], 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[97].

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[98].

These actions broadly reflect the consensus that emerged in the course of 2003, as confirmed at a public workshop held in October 2003[99]. Consensus in this area is all the more important since it is primarily for those interested parties, with the support of the 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

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

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

98 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.

99 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.

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?

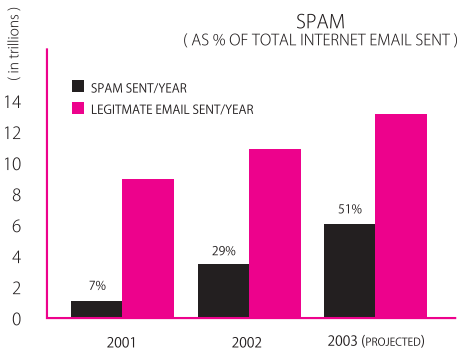
'Spam' is a term more often used than defined. In short, it is commonly used to describe unsolicited, often bulk e-mails. The new Directive does not define or use the term 'spam'. It uses the concepts of 'unsolicited communications' by 'electronic mail', 'for the purposes of direct marketing' which taken 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.



Source: IDC and Brightmail

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[100].

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.

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

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

statements[101]. Unfortunately all too many consumers do respond to these misleading or deceptive spam[102]. Pornographic messages can also be very upsetting[103]. Cleaning up mailboxes to remove spam is time-consuming for the user, and increases users' costs when filtering and other software facilities are needed.

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.

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 EUR just in terms of lost productivity[104]. 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 £[105]. 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[106].

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 Octo-

101 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)

102 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).

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

104 Source: Ferris Research, 2003.

105 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

106 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.

ber 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)[107]. This is the 'opt-in' system, which was until now only applicable to faxes and automated calling machines[108].

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[109].

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[110]. Consensus on these issues will avoid differences in interpretation that would damage the functioning of the internal market. Other aspects of unsolicited communications have been addressed in previous documents of the Working Party[111].

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

107 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.

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

109 Article 13(4) of Directive 2002/58/EC.

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

111 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

provisions on unsolicited communications[112].

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[113].

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[114].

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)[115]. 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[116]. 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

112 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.

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

114 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).

115 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).

116 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.

Directive on electronic commerce)[117].

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. 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[118]. 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[119]. The European Parliament has recently expressed its concern about this delay[120]. 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[121].

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;
- 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

117 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 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).

118 PROPOSAL FOR A COUNCIL FRAMEWORK DECISION ON ATTACKS AGAINST INFORMATION SYSTEMS, COM(2002) 173 FINAL, 19.4.2002.

119 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

120 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).

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

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[122]. 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.

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).

122 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.

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[123]. 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[124].

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.

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.

123 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

124 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

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[125]. 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[126].

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.

125 COM(2003) 443 final.

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

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 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[127].

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.

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

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

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[128].

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[129].

128 see http://www.ecp.nl/ projecten.php

129 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 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.

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[130]. 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.

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

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

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)[131]. 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.

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 seriously[132]. 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

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

132 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).

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 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[133].

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.

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[134].

133 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

134 See: http://www.dti.gov.uk/industries/ ecommunications/directive_on_privacy_electronic_communications_200258ec.html

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.

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.

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 tar-

geted. 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[135]. 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.

135 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.

Council Framework Decision 2005/222/ JHA of 24 February 2005 on attacks against information systems

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Articles 29, 30(1)(a), 31(1)(e) and 34(2)(b) thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Parliament [1],

Whereas:

(1) The objective of this Framework Decision is to improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States, through approximating rules on criminal law in the Member States in the area of attacks against information systems.

(2) There is evidence of attacks against information systems, in particular as a result of the threat from organised crime, and increasing concern at the potential of terrorist attacks against information systems which form part of the critical infrastructure of the Member States. This constitutes a threat to the achievement of a safer information society and an area of freedom, security and justice, and therefore requires a response at the level of the European Union.

(3) An effective response to those threats requires a comprehensive approach to network and information security, as underlined in the eEurope Action Plan, in the Communication by the Commission "Network and Information Security: Proposal for a European Policy Approach" and in the Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security [2].

(4) The need to further increase awareness of the problems related to information security and provide practical assistance has also been stressed in the European Parliament Resolution of 5 September 2001.

(5) Significant gaps and differences in Member States' laws in this area may hamper the fight against organised crime and terrorism, and may complicate effective police and judicial cooperation in the area of attacks against information systems. The transnational and borderless character of modern information systems means that attacks against such systems are often trans-border in nature, thus underlining the urgent need for further action to approximate criminal laws in this area.

(6) The Action Plan of the Council and the Commission on how to best implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice [3], the Tampere European Council on 15 to 16 October 1999, the Santa Maria da Feira European Council on 19 to 20 June 2000, the Commission in the "Scoreboard" and the European Parliament in its Resolution of 19 May 2000 indicate or call for legislative action against high technology crime, including common definitions, incriminations and sanctions.

(7) It is necessary to complement the work performed by international organisations, in particular the Council of Europe's work on approximating criminal law and the G8's work on transnational cooperation in the area of high tech crime, by providing a common approach in the European Union in this area. This call was further elaborated by the Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime".

(8) Criminal law in the area of attacks against information systems should be approximated in order to ensure the greatest possible police and judicial cooperation in the area of criminal offences related to attacks against information systems, and to contribute to the fight against organised crime and terrorism.

(9) All Member States have ratified the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data. The personal data processed in the context of the implementation of this Framework Decision should be protected in accordance with the principles of the said Convention.

(10) Common definitions in this area, particularly of information systems and computer data, are important to ensure a consistent approach in Member States in the application of this Framework Decision.

(11) There is a need to achieve a common approach to the constituent elements of criminal offences by providing for common offences of illegal access to an information system, illegal system interference and illegal data interference.

(12) In the interest of combating computer-related crime, each Member State should ensure effective judicial cooperation in respect of offences based on the types of conduct referred to in Articles 2, 3, 4 and 5.

(13) There is a need to avoid over-criminalisation, particularly of minor cases, as well as a need to avoid criminalising right-holders and authorised persons.

(14) There is a need for Member States to provide for penalties for attacks against information systems. The penalties thus provided for shall be effective, proportionate and dissuasive.

(15) It is appropriate to provide for more severe penalties when an attack against an information system is committed within the framework of a criminal organisation, as defined in the Joint Action 98/733 JHA of 21 December 1998 on making it a criminal offence to participate in a criminal organisation in the Member State of the European Union [4]. It is also appropriate to provide for more severe penalties where such an attack has caused serious damages or has affected essential interests.

(16) Measures should also be foreseen for the purposes of cooperation between Member States with a view to ensuring effective action against attacks against information systems. Member States should therefore make use of the existing network of operational contact points referred to in the Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime [5], for the exchange of information.

(17) Since the objectives of this Framework Decision, ensuring that attacks against information systems be sanctioned in all Member States by effective, proportionate and dissuasive criminal penalties and improving and encouraging judicial cooperation by removing potential complications, cannot be sufficiently achieved by the Member States, as rules have to be common and compatible, and can therefore be better achieved at the level of the Union, the Union

may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the EC Treaty. In accordance with the principle of proportionality, as set out in that Article, this Framework Decision does not go beyond what is necessary in order to achieve those objectives.

(18) This Framework Decision respects the fundamental rights and observes the principles recognised by Article 6 of the Treaty on European Union and reflected in the Charter of Fundamental Rights of the European Union, and notably Chapters II and VI thereof,

HAS ADOPTED THIS FRAMEWORK DECISION:

Article 1
Definitions

For the purposes of this Framework Decision, the following definitions shall apply:

(a) "information system" means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance;

(b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function;

(c) "legal person" means any entity having such status under the applicable law, except for States or other public bodies in the exercise of State authority and for public international organisations;

(d) "without right" means access or interference not authorised by the owner, other right holder of the system or part of it, or not permitted under the national legislation.

Article 2
Illegal access to information systems

1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.

2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.

Article 3
Illegal system interference

Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor.

Article 4
Illegal data interference

Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor.

Article 5
Instigation, aiding and abetting and attempt

1. Each Member State shall ensure that the instigation of aiding and abetting an offence referred to in Articles 2, 3 and 4 is punishable as a criminal offence.

2. Each Member State shall ensure that the attempt to commit the offences referred to in Articles 2, 3 and 4 is punishable as a criminal offence.

3. Each Member State may decide not to apply paragraph 2 for the offences referred to in Article 2.

Article 6
Penalties

1. Each Member State shall take the necessary measures to ensure that the offences referred to in Articles 2, 3, 4 and 5 are punishable by effective, proportional and dissuasive criminal penalties.

2. Each Member State shall take the necessary measures to ensure that the offences referred to in Articles 3 and 4 are punishable by criminal penalties of a maximum of at least between one and three years of imprisonment.

Article 7
Aggravating circumstances

1. Each Member State shall take the necessary measures to ensure that the offence referred to in Article 2(2) and the offence referred to in Articles 3 and 4 are punishable by criminal penalties of a maximum of at least between two and five years of imprisonment when committed within the framework of a criminal organisation as defined in Joint Action 98/733/JHA apart from the penalty level referred to therein.

2. A Member State may also take the measures referred to in paragraph 1 when the offence has caused serious damages or has affected essential interests.

Article 8
Liability of legal persons

1. Each Member State shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 2, 3, 4 and 5, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

   (a) a power of representation of the legal person, or

   (b) an authority to take decisions on behalf of the legal person, or

   (c) an authority to exercise control within the legal person.

2. Apart from the cases provided for in paragraph 1, Member States shall ensure that a legal person can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission of the offences referred to in Articles 2, 3, 4 and 5 for the benefit of that legal person by a person under its authority.

3. Liability of a legal person under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are involved as perpetrators, instigators or accessories in the commission of the offences referred to in Articles 2, 3, 4 and 5.

Article 9
Penalties for legal persons

1. Each Member State shall take the necessary measures to ensure that a legal person held liable pursuant to Article 8(1) is punishable by effective, proportionate and dissuasive penalties, which shall include criminal or non-criminal fines and may include other penalties, such as:

   (a) exclusion from entitlement to public benefits or aid;

   (b) temporary or permanent disqualification from the practice of commercial activities;

   (c) placing under judicial supervision; or

   (d) a judicial winding-up order.

2. Each Member State shall take the necessary measures to ensure that a legal person held liable pursuant to Article 8(2) is punishable by effective, proportionate and dissuasive penalties or measures.

Article 10
Jurisdiction

1. Each Member State shall establish its jurisdiction with regard to the offences referred to in Articles 2, 3, 4 and 5 where the offence has been committed:

   (a) in whole or in part within its territory; or

   (b) by one of its nationals; or

   (c) for the benefit of a legal person that has its head office in the territory of that Member State.

2. When establishing its jurisdiction in accordance with paragraph (1)(a), each Member State shall ensure that the jurisdiction includes cases where:

   (a) the offender commits the offence when physically present on its territory, whether or not the offence is against an information system on its territory; or

   (b) the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory.

3. A Member State which, under its law, does not as yet extradite or surrender its own nationals shall take the necessary measures to establish its jurisdiction over and to prosecute, where appropriate, the offences referred to in Articles 2, 3, 4 and 5, when committed by one of its nationals outside its territory.

4. Where an offence falls within the jurisdiction of more than one Member State and when any of the States concerned can validly prosecute

on the basis of the same facts, the Member States concerned shall cooperate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralising proceedings in a single Member State. To this end, the Member States may have recourse to any body or mechanism established within the European Union in order to facilitate cooperation between their judicial authorities and the coordination of their action. Sequential account may be taken of the following factors:

- the Member State shall be that in the territory of which the offences have been committed according to paragraph 1(a) and paragraph 2,
- the Member State shall be that of which the perpetrator is a national,
- the Member State shall be that in which the perpetrator has been found.

5. A Member State may decide not to apply, or to apply only in specific cases or circumstances, the jurisdiction rules set out in paragraphs 1(b) and 1(c).

6. Member States shall inform the General Secretariat of the Council and the Commission where they decide to apply paragraph 5, where appropriate with an indication of the specific cases or circumstances in which the decision applies.

Article 11
Exchange of information

1. For the purpose of exchange of information relating to the offences referred to in Articles 2, 3, 4 and 5, and in accordance with data protection rules, Member States shall ensure that they make use of the existing network of operational points of contact available 24 hours a day and seven days a week.

2. Each Member State shall inform the General Secretariat of the Council and the Commission of its appointed point of contact for the purpose of exchanging information on offences relating to attacks against information systems. The General Secretariat shall forward that information to the other Member States.

Article 12
Implementation

1. Member States shall take the necessary measures to comply with the provisions of this Framework Decision by 16 March 2007.

2. By 16 March 2007 Member States shall transmit to the General Secretariat of the Council and to the Commission the text of any provisions transposing into their national law the obligations imposed on them under this Framework Decision. By 16 September 2007, on the basis of a report established on the basis of information and a written report by the Commission, the Council shall assess the extent to which Member States have complied with the provisions of this Framework Decision.

Article 13
Entry into force

This Framework Decision shall enter into force on the date of its publication in the Official Journal of the European Union.

Done at Brussels, 24 February 2005.

For the Council

The President N. Schmit

[1] OJ C 300 E, 11.12.2003, p. 26.

[2] OJ C 43, 16.2.2002, p. 2.

[3] OJ C 19, 23.1.1999, p. 1.

[4] OJ L 351, 29.12.1998, p. 1.

[5] OJ C 187, 3.7.2001, p. 5.

Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 153(2) thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Economic and Social Committee [1],

After consulting the Committee of the Regions,

Acting in accordance with the procedure laid down in Article 251 of the Treaty [2],

Whereas:

(1) Internet penetration and the use of new technologies such as mobile phones are still growing considerably in the Community. Alongside this, dangers, especially for children, and abuse of those technologies continue to exist, and new dangers and abuses are emerging. In order to encourage the exploitation of the opportunities offered by the Internet and new online technologies, measures are also needed to promote their safer use and protect the end-user from unwanted content.

(2) The eEurope 2005 Action Plan, developing the Lisbon strategy, aims to stimulate secure services, applications and content based on a widely available broadband infrastructure. Among its objectives, are a secure information infrastructure, the development, analysis and dissemination of best practices, benchmarking and a coordination mechanism for e-policies.

(3) The legislative framework being established at Community level to deal with the challenges of digital content in the Information Society now includes rules relating to online services, notably those on unsolicited commercial e-mail in the Directive on privacy and electronic communications [3] and on important aspects of the liability of intermediary service providers in the Directive on electronic commerce [4], and recommendations for Member States, the industry and parties concerned and the Commission, together with the indicative guidelines on the protection of minors, in Recommendation 98/560/EC [5].

(4) There will be a continued need for action both in the area of content which is potentially harmful to children or unwanted by the end-user and in the area of illegal content, in particular child pornography and racist material.

(5) Reaching international agreement on legally binding basic rules is desirable but will not be easily achieved. Even if such agreement is reached, it will not be enough in itself to ensure that the rules are implemented or that those at risk are protected.

(6) The Safer Internet Action Plan (1999 to 2004) adopted by Decision No 276/1999/EC [6] has provided Community financing, which has successfully encouraged a variety of initiatives and has given European added value. Further funding will help new initiatives to build on the work already accomplished.

(7) Practical measures are still needed to encourage reporting of illegal content to those in a position to deal with it, to encourage assessment of the performance of filter technologies and the benchmarking of those technologies, to spread best practice for codes of conduct embodying generally agreed canons of behaviour, and to inform and educate parents and children on the best way to benefit from the potential of new online technologies in a safe way.

(8) Action at Member State level involving a wide range of actors from national, regional and local government, network operators, parents, teachers and school administrators is essential. The Community can stimulate best practice in Member States by carrying out an orientation role both within the European Union and internationally and providing support for European-level benchmarking, networking and applied research.

(9) International cooperation is also essential and can be stimulated, coordinated, relayed and implemented by action through the Community

networking structures.

(10) The measures that the Commission is empowered to adopt under the implementing powers, conferred on it by this Decision, are essentially management measures relating to the implementation of a programme with substantial budgetary implications within the meaning of Article 2(a) of Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission [7]. Those measures should therefore be adopted in accordance with the management procedure provided for in Article 4 of that Decision.

(11) The Commission should ensure complementarity and synergy with related Community initiatives and programmes, including, inter alia, by taking into account the work performed by other bodies.

(12) This Decision lays down, for the entire duration of the programme, a financial framework constituting the prime reference, within the meaning of point 33 of the Interinstitutional Agreement of 6 May 1999 between the European Parliament, the Council and the Commission on budgetary discipline and improvement of the budgetary procedure [8], for the budgetary authority during the annual budgetary procedure.

(13) Since the objectives of this Decision, namely to promote safer use of the Internet and new online technologies and to fight against illegal content and content unwanted by the end-user, cannot be sufficiently achieved by the Member States owing to the transnational character of the issues at stake and can, therefore, by reason of the European scale and effects of the actions, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Decision does not go beyond what is necessary in order to achieve those objectives.

(14) This Decision respects the fundamental rights and observes the principles reflected in the Charter of Fundamental Rights of the European Union, in particular Articles 7 and 8 thereof,

HAVE DECIDED AS FOLLOWS:

Article 1
Objective of the programme

1. This Decision establishes a Community programme for the period 2005 to 2008 to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end-user.

   The programme shall be known as the "Safer Internet plus" programme (hereinafter the programme).

2. In order to attain the aims of the programme referred to in paragraph 1, the following actions shall be addressed:

   (c) fighting against illegal content;

   (d) tackling unwanted and harmful content;

   (e) promoting a safer environment;

   (f) awareness-raising.

The activities to be carried out under those actions are set out in Annex I.

The programme shall be implemented in accordance with Annex III.

Article 2
Participation

1. Participation in the programme shall be open to legal entities established in the Member States.

   Participation shall also be open to legal entities established in the candidate countries in accordance with bilateral agreements in existence or to be concluded with those countries.

2. Participation in the programme may be opened to legal entities established in EFTA States which are contracting parties to the EEA Agreement, in accordance with the provisions of Protocol 31 to that Agreement.

3. Participation in the programme may be opened, without financial support by the Community under the programme, to legal entities established in third countries and to international organisations, where such participation contributes effectively to the implementation of the programme. The decision to allow such participation shall be adopted in accordance with the procedure referred to in Article 4(2).

Article 3
Competences of the Commission

1. The Commission shall be responsible for the implementation of the programme.
2. The Commission shall draw up a work programme on the basis of this Decision.
3. In the implementation of the programme, the Commission shall, in close cooperation with the Member States, ensure that it is generally consistent with and complementary to other relevant Community policies, programmes and actions, in particular the Community research and technological development programmes and the Daphne II [9], Modinis [10] and eContentplus [11] programmes.
4. The Commission shall act in accordance with the procedure referred to in Article 4(2) for the purposes of the following:
   (a) adoption and modifications of the work programme;
   (b) breakdown of budgetary expenditure;
   (c) determination of the criteria and content of calls for proposals, in accordance with the objectives set out in Article 1;
   (d) assessment of the projects proposed following calls for proposals for Community funding where the estimated Community contribution is equal to, or more than, EUR 500000;
   (e) any departure from the rules set out in Annex III;
   (f) implementation of measures for evaluating the programme.
5. The Commission shall inform the Committee referred to in Article 4 of progress with the implementation of the programme.

Article 4
Committee

1. The Commission shall be assisted by a Committee.
2. Where reference is made to this paragraph, Articles 4 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

   The period laid down in Article 4(3) of Decision 1999/468/EC shall be set at three months.

   The Committee shall adopt its rules of procedure.

Article 5
Monitoring and evaluation

1. In order to ensure that Community aid is used efficiently, the Commission shall ensure that actions under this Decision are subject to prior appraisal, follow-up and subsequent evaluation.
2. The Commission shall monitor the implementation of projects under the programme. The Commission shall evaluate the manner in which the projects have been carried out and the impact of their implementation in order to assess whether the original objectives have been achieved.
3. The Commission shall report on the implementation of the actions referred to in Article 1(2) to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, by mid-2006 at the latest. In this context, the Commission shall report on the consistency of the amount for 2007 to 2008 with the financial perspective. If applicable, the Commission shall take the necessary steps within the budgetary procedures for 2007 to 2008 to ensure the consistency of the annual appropriations with the financial perspective.

   The Commission shall submit a final evaluation report at the end of the programme.
4. The Commission shall forward the results of its quantitative and qualitative evaluations to the European Parliament and the Council together with any appropriate proposals for the amendment of this Decision. The results shall be forwarded before presentation of the draft general budget of the European Union for the years 2007 and 2009 respectively.

Article 6
Financial provisions

1. The financial framework for the implementation of the Community actions under this Decision for the period from 1 January 2005 to 31 December 2008 is hereby set at EUR 45 million, of which EUR 20050000 is for the period until 31 December 2006.

   For the period following 31 December 2006, the amount shall be deemed to be confirmed if it is consistent for this phase with the financial perspective in force for the period commencing in 2007.

   The annual appropriations for the period from

2005 to 2008 shall be authorised by the budgetary authority within the limits of the financial perspective.

2. An indicative breakdown of expenditure is given in Annex II.

Article 7
Entry into force

This Decision shall enter into force on the date of its publication in the Official Journal of the European Union.

Done at Strasbourg, 11 May 2005.
For the European Parliament
The President J. P. Borrel1 Fontelles
For the Council
The President N. Schmit

[1] Opinion of 16 December 2004 (not yet published in the Official Journal).

[2] Opinion of the European Parliament of 2 December 2004 (not yet published in the Official Journal) and Council Decision of 12 April 2005.

[3] 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 (OJ L 201, 31.7.2002, p. 37).

[4] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178, 17.7.2000, p. 1).

[5] Council Recommendation 98/560/EC of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity (OJ L 270, 7.10.1998, p. 48).

[6] Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a Multiannual Community Action Plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors (OJ L 33, 6.2.1999, p. 1). Decision as last amended by Decision No 787/2004/EC (OJ L 138, 30.4.2004, p. 12).

[7] OJ L 184, 17.7.1999, p. 23.

[8] OJ C 172, 18.6.1999, p. 1. Agreement as amended by Decision 2003/429/EC of the European Parliament and of the Council (OJ L 147, 14.6.2003, p. 25).

[9] Decision No 803/2004/EC of the European Parliament and of the Council of 21 April 2004 adopting a programme of Community action (2004 to 2008) to prevent and combat violence against children, young people and women and to protect victims and groups at risk (the Daphne II programme) (OJ L 143, 30.4.2004, p. 1).

[10] Decision No 2256/2003/EC of the European Parliament and of the Council of 17 November 2003 adopting a multiannual programme (2003-2005) for the monitoring of the eEurope 2005 action plan, dissemination of good practices and the improvement of network and information security (Modinis) (OJ L 336, 23.12.2003, p. 1). Decision as amended by Decision No 787/2004/EC.

[11] Decision No 456/2005/EC of the European Parliament and of the Council of 9 March 2005 establishing a multiannual Community programme to make digital content in Europe more accessible, usable and exploitable (OJ L 79, 24.3.2005, p. 1).

ANNEX I

ACTIONS

1. ACTION 1: FIGHTING AGAINST ILLEGAL CONTENT

Hotlines allow members of the public to report illegal content. They pass the reports on to the appropriate body (an Internet Service Provider (ISP), the police or a correspondent hotline) for action. Civilian hotlines complement police hotlines, where these exist. Their role is distinct from that of the law enforcement authorities, since they do not investigate offences or arrest or prosecute offenders. They may constitute centres of expertise providing guidance to ISPs as to what content might be illegal.

The existing hotline network is a unique structure that would not have been set up without Community funding. As pointed out in the 2002 evaluation report for the Safer Internet Action Plan, the network has been very successful in expanding membership and has an international reach. In order for the hotlines to develop their full potential, it is necessary to ensure Europe-wide coverage and cooperation, and to increase effectiveness through exchange of information, best practice and experience. Community funds should also be used to raise public awareness of the hotlines, thereby making them more effective.

Funding will be provided for hotlines, selected following a call for proposals, to act as nodes of the network and to cooperate with the other nodes within the European network of hotlines.

If necessary, telephone helplines could be supported, where children could raise concerns about illegal and harmful content on the Internet.

For the purpose of evaluating the effectiveness of hotlines, several indicators should be taken into account. Qualitative and quantitative data should be collected on the establishment and opera-

tion of hotlines, the number of national nodes, the geographical coverage in the Member States, the number of reports received, the number and level of experience of hotline staff, the reports forwarded for action to the public authorities and ISPs, and, to the extent available, action taken as a result, in particular the number and kind of web pages withdrawn by ISPs as a result of information provided by the hotlines. Those data should be made public if possible and should be forwarded to the competent authorities.

To ensure that the programme is effective, hotlines are required in all Member States and candidate countries where none currently exist. These new hotlines must be incorporated quickly and effectively into the existing European network of hotlines. Incentives must be given to speed up the process of setting up hotlines. Links between this network and hotlines in third countries (particularly in other European countries where illegal content is hosted and produced) should be promoted, enabling common approaches to be developed and know-how and best practice to be transferred. In accordance with national legislation, and where appropriate and necessary, mechanisms for cooperation between civilian hotlines and law enforcement authorities must be further improved, including, for example, the development of codes of conduct for such hotlines. Where appropriate, there may be a need for hotline staff to receive legal and technical training. Active participation by hotlines in networking and cross-border activities will be mandatory.

Hotlines should be linked to Member State initiatives, supported at national level and should be financially viable to ensure continued operation beyond the duration of this Programme. Co-funding is intended for civilian hotlines and therefore will not be provided for hotlines run by the police. Hotlines will make clear to users the difference between their activities and those of public authorities, and will inform them of the existence of alternative ways of reporting illegal content.

In order to achieve maximum impact and effectiveness with available funding, the hotline network must operate as efficiently as possible. This can best be achieved by assigning a coordinating node to the network, which will facilitate agreement between the hotlines so as to develop European-level guidelines, working methods and practices which respect the limits of the national laws applying to the individual hotlines.

The coordinating node will:

- promote the network as a whole, so as to generate European-level visibility and raise public awareness thereof throughout the European Union, providing e.g. a single identity and entry point giving straightforward access to the appropriate national contact,
- make contact with appropriate bodies with a view to completing the network's coverage in the Member States and candidate countries,
- improve the operational effectiveness of the network,
- draw up best practice guidelines for hotlines and adapt them to new technology,
- organise regular exchanges of information and experience between hotlines,
- provide a pool of expertise for advice and a coaching process for start-up hotlines, particularly in candidate countries,
- ensure liaison with hotlines in third countries,
- maintain a close working relationship with the awareness-raising coordinating node (see point 4 below) so as to ensure the cohesion and effectiveness of overall programme operations and increase public awareness of the hotlines,
- participate in the Safer Internet Forum and other relevant events, coordinating input/feedback from hotlines.

The coordinating node will monitor the effectiveness of hotlines and collect accurate and meaningful statistics on their operation (number and type of reports received, action taken and result, etc.). These statistics should be comparable across Member States.

The hotline network should ensure coverage of and the exchange of reports on the major types of illegal content of concern — extending beyond the area of child pornography. Different mechanisms and expertise may be required to deal with other areas such as racist content, which might involve other types of node dealing with the various issues. Since the financial and administrative resources of the programme are limited, not all such nodes would necessarily receive funding, which might have to be concentrated on a reinforced role for the coordinating node in those areas.

2. ACTION 2: TACKLING UNWANTED AND HARMFUL CONTENT

In addition to action to fight illegal content at its source, users, responsible adults where the users are minors, may need technical tools. Accessibility to these tools may be promoted in order to enable users to make their own decisions on how to deal with unwanted and harmful content (user empowerment).

Further funding should be provided to increase the information available on the performance and effectiveness of filtering software and services to allow users to make an informed choice. User organisations and scientific research institutes can be valuable partners in this effort.

Rating systems and quality labels, in combination with filtering technologies, can help to enable users to select the content they wish to receive and provide European parents and educators with the necessary information to make decisions in accordance with their cultural and linguistic values. Taking account of the results of previous projects, funding could be given to projects which aim to adapt rating systems and quality labels to take account of the convergence of telecommunications, audio-visual media and information technology and to self-regulatory initiatives to back up the reliability of self-labelling and services for assessing the accuracy of self-rating labels. Further work may also be needed to encourage take-up of rating systems and quality labels by content providers.

It would be desirable to try to take account of safe use by children when developing new technologies, instead of trying to deal with any consequences of the new technologies after they have been devised. The safety of the end-user is a criterion to be taken into account along with technical and commercial considerations. One way of doing this would be to foster an exchange of views between child welfare specialists and technical experts. However, account should be taken of the fact that not every product developed for the online world is intended for use by children.

The programme will therefore provide funding for technological measures which meet the needs of users and enable them to limit the amount of unwanted and harmful content, and manage the unwanted spam, which they receive, including:

- assessing the effectiveness of available filtering technology and providing this information to the public in a clear, simple way that facilitates comparison,
- facilitating and coordinating exchanges of information and best practices on effective ways of tackling unwanted and harmful content,
- increasing take-up of content rating and quality site labels by content providers and adapting content rating and labels to take account of the availability of the same content through different delivery mechanisms (convergence),
- if necessary, contributing to the accessibility of filter technology notably in languages not adequately covered by the market. Where appropriate, the technologies used should safeguard the right to privacy pursuant to Directives 95/46/EC [1] and 2002/58/EC.

The use of technological measures which enhance privacy will be encouraged. Activities under this action will take fully into account the provisions of Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems [2].

Implementation of this action will be closely coordinated with the actions on promoting a safer environment (self-regulatory action) and awareness-raising (informing the public about how to deal with unwanted and harmful content).

3. ACTION 3: PROMOTING A SAFER ENVIRONMENT

A fully functioning system of self-regulation is an essential element in limiting the flow of unwanted, harmful and illegal content. Self-regulation involves a number of components: consultation and appropriate representation of the parties concerned; codes of conduct; national bodies facilitating cooperation at Community level; and national evaluation of self-regulation frameworks [3]. There is a continuing need for Community work in this area to encourage the European Internet and new online technologies industries to implement codes of conduct.

The Safer Internet Forum developed in 2004 under the Safer Internet Action Plan is to become a discussion forum including representatives of industry, law enforcement authorities, policy-makers and user organisations (e.g. parent and teacher organisations, child protection groups, consumer protection bodies and civil and digital rights organisations). It will

provide a platform for national co-regulatory or self-regulatory bodies to exchange experience and an opportunity to discuss ways in which industry can contribute to the fight against illegal content.

The Safer Internet Forum will provide a focal point for discussion at expert level and a platform to drive consensus, inputting conclusions, recommendations, guidelines etc. to relevant national and European channels.

The Safer Internet Forum will span all the actions, facilitating discussion and stimulating action relevant to illegal, unwanted and harmful content. Consisting of plenary sessions and, where necessary for specific issues, working groups with clear objectives and deadlines, it will be a meeting place for actors from all areas, including government agencies and programmes, standards bodies, industry, services within the Commission and user organisations (e.g. parent and teacher organisations, child protection groups, consumer protection bodies and civil and digital rights organisations). The Forum will provide an opportunity for people, active at national and European level, especially those involved in Member State programmes and initiatives, to exchange views, information and experience. Where appropriate, the Safer Internet Forum should exchange information and cooperate with relevant organisations active in related areas, such as network and information security.

The Safer Internet Forum will have the specific objectives of:

1. stimulating networking of the appropriate structures within Member States and developing links with self-regulatory bodies outside Europe;
2. stimulating consensus and self-regulation on issues such as quality rating of websites, cross-media content rating, rating and filtering techniques, extending them to new forms of content such as online games and new forms of access such as mobile phones;
3. encouraging service providers to draw up codes of conduct on issues such as handling notice and take down procedures in a transparent and conscientious manner and informing users about safer use of Internet and the existence of hotlines for reporting illegal content;
4. promoting research into the effectiveness of rating projects and filtering technologies. User organisations and scientific research institutes can be valuable partners in this effort.

Results and findings from ongoing and completed projects co-funded by the programme will feed into the process. By providing an open platform, the Forum will help to raise levels of awareness and attract the involvement of the candidate countries and other third countries, providing an international arena to address a global problem. It will, therefore, ensure that key associations, such as user organisations (e.g. parent and teacher organisations, child protection groups, consumer protection bodies and civil and digital rights organisations), industries and public bodies are aware of, are consulted on and contribute to safer-use initiatives within the Community and internationally.

Participation in the Safer Internet Forum will be open to interested parties from outside the Community and candidate countries. International co-operation will be enhanced by a round table linked to the Forum in order to ensure regular dialogue on best practice, codes of conduct, self-regulation and quality ratings. The Commission will ensure that synergies with related fora and similar initiatives are fully exploited.

A call for tenders may be organised in order to provide a secretariat to support the Safer Internet Forum, including subject-field experts, to suggest themes of study, prepare working papers, moderate discussions and record conclusions.

A further type of activity attracting financial support at Community level could for instance include self-regulatory projects to devise cross-border codes of conduct. Advice and assistance may be provided so as to ensure cooperation at Community level through networking of the appropriate bodies within Member States and candidate countries and through systematic review and reporting of relevant legal and regulatory issues, to help develop methods of assessment and certification of self-regulation, to provide practical assistance to countries wishing to set up self-regulatory bodies and to expand links with self-regulatory bodies outside Europe.

4. ACTION 4: AWARENESS-RAISING

Awareness-raising actions should address a range of categories of illegal, unwanted and harmful content (including, for example, content considered unsuitable for children and racist and xenophobic content) and, where appropriate, take into account related issues of consumer protection, data protection and information and network security (viruses/spam). They should deal with content distributed over the World Wide Web as well as new forms of in-

teractive information and communication brought about by the rapid spread of the Internet and mobile telephony (e.g. peer-to-peer services, broadband video, instant messaging, chatrooms, etc.).

The Commission will continue to take steps to encourage cost-effective means of distribution of information to large numbers of users, notably by using multiplier organisations and electronic dissemination channels, so as to reach the intended target groups. The Commission could consider in particular the use of mass media and distribution of information material to schools and Internet cafés.

The programme will provide support to appropriate bodies, which will be selected following an open call for proposals to act as awareness-raising nodes in each Member State and candidate country and, which will carry out awareness-raising actions and programmes in close cooperation with all relevant actors at national, regional and local levels. European added value will be provided by a coordinating node, which will liaise closely with other nodes to ensure that best practice is exchanged.

Bodies seeking to act as awareness-raising nodes will need to show that they have the strong support of national authorities. They should have a clear mandate to educate the public in safer use of the Internet and new online technologies or in media and information literacy, and must have the necessary financial resources to implement that mandate.

Awareness-raising nodes will be expected to:

- devise a cohesive, hard-hitting and targeted awareness-raising campaign using the most appropriate media, taking into account best practice and experience in other countries,
- establish and maintain a partnership (formal or informal) with key players (government agencies, press and media groups, ISP associations, user organisations, education stakeholders) and actions in their country relating to safer use of the Internet and new online technologies,
- promote dialogue and exchange of information notably between stakeholders from the education and technological fields,
- where appropriate, cooperate with work in areas related to this programme such as in the wider fields of media and information literacy or consumer protection,
- inform users about European filtering software and services and about hotlines and self-regulation schemes,
- actively cooperate with other national nodes in the European network by exchanging information about best practices, participating in meetings and designing and implementing a European approach, adapted as necessary for national linguistic and cultural preferences,
- provide a pool of expertise and technical assistance to start up awareness-raising nodes (new nodes could be "adopted" by a more experienced node).

To ensure maximum cooperation and effectiveness, the coordinating node will be funded to provide logistical and infrastructural support for nodes in each Member State, ensuring European-level visibility, good communication and exchange of experience so that lessons learnt can be applied on an ongoing basis (for instance by adapting material used for raising public awareness).

The coordinating node should:

- provide effective communication and ensure that information and best practice are exchanged within the network,
- provide training in safer use of the Internet and new online technologies for the staff of awareness-raising nodes (training for trainers),
- provide technical assistance to candidate countries wishing to set up awareness-raising actions,
- coordinate the provision by awareness-raising nodes of expertise and technical assistance to start up awareness-raising nodes,
- propose indicators and manage the collection, analysis and exchange of statistical information about awareness-raising activities, so as to assess their impact,
- provide infrastructure for a single, comprehensive transnational repository (web portal) of relevant information and awareness-raising and research resources with localised content (or local subsites, as appropriate), which may include news snippets, articles and monthly newsletters in several languages, and provide visibility for Safer Internet Forum activities,
- expand links with awareness-raising activities

outside Europe,

- participate in the Safer Internet Forum and other relevant events, coordinating input/ feedback from the awareness-raising network.

Research will also be carried out on a comparable basis into the way people, especially children, use new online technologies. Further action at Community level could for instance include support for specific child-friendly Internet services or an award for the best awareness-raising activity of the year.

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31). Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

[2] OJ L 69, 16.3.2005, p. 67.

[3] See the indicative guidelines for the implementation, at national level, of a self-regulation framework for the protection of minors and human dignity in online audiovisual and information services in Recommendation 98/560/EC.

ANNEX II

INDICATIVE BREAKDOWN OF EXPENDITURE

1. Fighting against illegal content
   25 - 30 %
2. Tackling unwanted and harmful content
   10 - 17 %
3. Promoting a safer environment
   8 - 12 %
4. Awareness-raising
   47 - 51 %

ANNEX III

THE MEANS FOR IMPLEMENTING THE PROGRAMME

1. The Commission will implement the programme in accordance with the technical content specified in Annex I.
2. The programme will be executed through indirect action comprising:

(g) shared-cost actions

(i) Pilot projects and best-practice actions. Ad hoc projects in areas relevant to the programme, ncluding projects demonstrating best practice or involving innovative uses of existing technology.

(ii) Networks: networks bringing together a variety of stakeholders to ensure action throughout the European Union and to facilitate coordination activities and the transfer of knowledge. They may be linked to best-practice actions.

(iii) Applied Europe-wide research carried out on a comparable basis into the way people, especially children, use new online technologies.

Community funding will normally not exceed 50 % of the cost of the project. Public sector bodies may be reimbursed on the basis of 100 % of the additional costs;

(h) accompanying measures

The following accompanying measures will contribute to the implementation of the programme or the preparation of future activities.

(i) Benchmarking and opinion surveys to produce reliable data on safer use of the Internet and new online technologies for all Member States collected through a comparable methodology.

(ii) Technical assessment of technologies, such as filtering, designed to promote safer use of the Internet and new online technologies. The assessment will also take into account whether or not these technologies enhance privacy.

(iii) Studies in support of the programme and its actions, including self-regulation and the work of the Safer Internet Forum, or the preparation of future activities.

(iv) Prize competitions for best practice.

(v) Exchange of information, conferences, seminars, workshops or other meetings and the management of clustered activities.

(vi) Dissemination, information and communication activities.

Measures devoted to the commercialisation of products, processes or services, marketing activities and sales promotion are excluded.

3. The selection of shared-cost actions will be based on calls for proposals published on the Commission's Internet site in accordance with the financial provisions in force.

4. Applications for Community support should provide, where appropriate, a financial plan listing all the components of the funding of the projects, including the financial support requested from the Community, and any other requests for or grants of support from other sources.

5. Accompanying measures will be implemented through calls for tenders in accordance with the financial provisions in force.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the Opinion of the European Economic and Social Committee [1],

Acting in accordance with the procedure laid down in Article 251 of the Treaty [2],

Whereas:

(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [3] requires Member States to protect the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.

(2) 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 elec-

tronic communications) [4] translates the principles set out in Directive 95/46/EC into specific rules for the electronic communications sector.

(3) Articles 5, 6 and 9 of Directive 2002/58/EC lay down the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. Such data must be erased or made anonymous when no longer needed for the purpose of the transmission of a communication, except for the data necessary for billing or interconnection payments. Subject to consent, certain data may also be processed for marketing purposes and the provision of value-added services.

(4) Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.

(5) Several Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences. Those national provisions vary considerably.

(6) The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and location data to be retained and the conditions and periods of retention.

(7) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime.

(8) The Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.

(9) Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, inter alia, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR is therefore a necessary measure.

(10) On 13 July 2005, the Council reaffirmed in its declaration condemning the terrorist attacks on London the need to adopt common measures on the retention of telecommunications data as soon as possible.

(11) Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.

(12) Article 15(1) of Directive 2002/58/EC continues to apply to data, including data relating to unsuccessful call attempts, the retention of which is not specifically required under this Directive and which therefore fall outside the scope thereof, and to retention for purposes, including judicial purposes, other than those covered by this Directive.

(13) This Directive relates only to data generated

or processed as a consequence of a communication or a communication service and does not relate to data that are the content of the information communicated. Data should be retained in such a way as to avoid their being retained more than once. Data generated or processed when supplying the communications services concerned refers to data which are accessible. In particular, as regards the retention of data relating to Internet e-mail and Internet telephony, the obligation to retain data may apply only in respect of data from the providers' or the network providers' own services.

(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve. In order to obtain advice and encourage the sharing of experience of best practice in these matters, the Commission intends to establish a group composed of Member States' law enforcement authorities, associations of the electronic communications industry, representatives of the European Parliament and data protection authorities, including the European Data Protection Supervisor.

(15) Directive 95/46/EC and Directive 2002/58/EC are fully applicable to the data retained in accordance with this Directive. Article 30(1)(c) of Directive 95/46/EC requires the consultation of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of that Directive.

(16) The obligations incumbent on service providers concerning measures to ensure data quality, which derive from Article 6 of Directive 95/46/EC, and their obligations concerning measures to ensure confidentiality and security of processing of data, which derive from Articles 16 and 17 of that Directive, apply in full to data being retained within the meaning of this Directive.

(17) It is essential that Member States adopt legislative measures to ensure that data retained under this Directive are provided to the competent national authorities only in accordance with national legislation in full respect of the fundamental rights of the persons concerned.

(18) In this context, Article 24 of Directive 95/46/EC imposes an obligation on Member States to lay down sanctions for infringements of the provisions adopted pursuant to that Directive. Article 15(2) of Directive 2002/58/EC imposes the same requirement in relation to national provisions adopted pursuant to Directive 2002/58/EC. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems [5] provides that the intentional illegal access to information systems, including to data retained therein, is to be made punishable as a criminal offence.

(19) The right of any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with national provisions adopted pursuant to Directive 95/46/EC to receive compensation, which derives from Article 23 of that Directive, applies also in relation to the unlawful processing of any personal data pursuant to this Directive.

(20) The 2001 Council of Europe Convention on Cybercrime and the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data also cover data being retained within the meaning of this Directive.

(21) Since the objectives of this Directive, namely to harmonise the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Directive, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(22) This Directive respects the fundamental rights and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union. In particular, this Directive, together with Directive 2002/58/EC, seeks to ensure full compliance with citizens' fundamental rights to respect for private life and communications and to the protection of their personal data, as enshrined in Articles 7 and 8 of the Charter.

(23) Given that the obligations on providers of electronic communications services should be proportionate, this Directive requires that they retain only such data as are generated or processed in the process of supplying their communications services. To the extent that such data are not generated or processed by those pro-

viders, there is no obligation to retain them. This Directive is not intended to harmonise the technology for retaining data, the choice of which is a matter to be resolved at national level.

(24) In accordance with paragraph 34 of the Interinstitutional agreement on better law-making [6], Member States are encouraged to draw up, for themselves and in the interests of the Community, their own tables illustrating, as far as possible, the correlation between this Directive and the transposition measures, and to make them public.

(25) This Directive is without prejudice to the power of Member States to adopt legislative measures concerning the right of access to, and use of, data by national authorities, as designated by them. Issues of access to data retained pursuant to this Directive by national authorities for such activities as are referred to in the first indent of Article 3(2) of Directive 95/46/EC fall outside the scope of Community law. However, they may be subject to national law or action pursuant to Title VI of the Treaty on European Union. Such laws or action must fully respect fundamental rights as they result from the common constitutional traditions of the Member States and as guaranteed by the ECHR. Under Article 8 of the ECHR, as interpreted by the European Court of Human Rights, interference by public authorities with privacy rights must meet the requirements of necessity and proportionality and must therefore serve specified, explicit and legitimate purposes and be exercised in a manner that is adequate, relevant and not excessive in relation to the purpose of the interference,

HAVE ADOPTED THIS DIRECTIVE:

Article 1
Subject matter and scope

1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Article 2
Definitions

1. For the purpose of this Directive, the definitions in Directive 95/46/EC, in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [7], and in Directive 2002/58/EC shall apply.

2. For the purpose of this Directive:

   (a) "data" means traffic data and location data and the related data necessary to identify the subscriber or user;

   (b) "user" means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;

   (c) "telephone service" means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services);

   (d) "user ID" means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service;

   (e) "cell ID" means the identity of the cell from which a mobile telephony call originated or in which it terminated;

   (f) "unsuccessful call attempt" means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.

Article 3
Obligation to retain data

1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or proc-

essed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.

Article 4
Access to data

Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.

Article 5
Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

   (a) data necessary to trace and identify the source of a communication:

      (1) concerning fixed network telephony and mobile telephony:

         (i) the calling telephone number;

         (ii) the name and address of the subscriber or registered user;

      (2) concerning Internet access, Internet e-mail and Internet telephony:

         (i) the user ID(s) allocated;

         (ii) the user ID and telephone number allocated to any communication entering the public telephone network;

         (iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

   (b) data necessary to identify the destination of a communication:

      (1) concerning fixed network telephony and mobile telephony:

         (i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

         (ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

      (2) concerning Internet e-mail and Internet telephony:

         (i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

         (ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

   (c) data necessary to identify the date, time and duration of a communication:

      (1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

      (2) concerning Internet access, Internet e-mail and Internet telephony:

         (i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

(3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

(f) data necessary to identify the location of mobile communication equipment:

(1) the location label (Cell ID) at the start of the communication;

(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

Article 6
Periods of retention

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Article 7
Data protection and data security

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:

(a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;

and

(d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

Article 8
Storage requirements for retained data

Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.

Article 9
Supervisory authority

1. Each Member State shall designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7 regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC.

2. The authorities referred to in paragraph 1 shall act with complete independence in carrying out the monitoring referred to in that paragraph.

Article 10
Statistics

1. Member States shall ensure that the Commission is provided on a yearly basis with statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network. Such statistics shall include:

   - the cases in which information was provided to the competent authorities in accordance with applicable national law,
   - the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data,
   - the cases where requests for data could not be met.

2. Such statistics shall not contain personal data.

Article 11
Amendment of Directive 2002/58/EC

The following paragraph shall be inserted in Article 15 of Directive 2002/58/EC:

"1a. Paragraph 1 shall not apply to data specifically required by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks [] to be retained for the purposes referred to in Article 1(1) of that Directive.

Aricle 12
Future measures

1. A Member State facing particular circumstances that warrant an extension for a limited period of the maximum retention period referred to in Article 6 may take the necessary measures. That Member State shall immediately notify the Commission and inform the other Member States of the measures taken under this Article and shall state the grounds for introducing them.

2. The Commission shall, within a period of six months after the notification referred to in paragraph 1, approve or reject the national measures concerned, after having examined whether they are a means of arbitrary discrimination or a disguised restriction of trade between Member States and whether they constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within that period the national measures shall be deemed to have been approved.

3. Where, pursuant to paragraph 2, the national measures of a Member State derogating from the provisions of this Directive are approved, the Commission may consider whether to propose an amendment to this Directive.

Article 13
Remedies, liability and penalties

1. Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive.

2. Each Member State shall, in particular, take the necessary measures to ensure that any intentional access to, or transfer of, data retained in accordance with this Directive that is not permitted under national law adopted pursuant to this Directive is punishable by penalties, including administrative or criminal penalties, that are effective, proportionate and dissuasive.

Article 14
Evaluation

1. No later than 15 September 2010, the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers, taking into account further developments in electronic communi-

cations technology and the statistics provided to the Commission pursuant to Article 10 with a view to determining whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data in Article 5 and the periods of retention provided for in Article 6. The results of the evaluation shall be made public.

2. To that end, the Commission shall examine all observations communicated to it by the Member States or by the Working Party established under Article 29 of Directive 95/46/EC.

Article 15
Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by no later than 15 September 2007. They shall forthwith inform the Commission thereof. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

3. Until 15 March 2009, each Member State may postpone application of this Directive to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail. Any Member State that intends to make use of this paragraph shall, upon adoption of this Directive, notify the Council and the Commission to that effect by way of a declaration. The declaration shall be published in the Official Journal of the European Union.

Article 16
Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

Article 17
Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 15 March 2006.

For the European Parliament
The President J. Borrell Fontelles
For the Council
The President H. Winkler

[1] Opinion delivered on 19 January 2006 (not yet published in the Official Journal).

[2] Opinion of the European Parliament of 14 December 2005 (not yet published in the Official Journal) and Council Decision of 21 February 2006.

[3] OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

[4] OJ L 201, 31.7.2002, p. 37.

[5] OJ L 69, 16.3.2005, p. 67.

[6] OJ C 321, 31.12.2003, p. 1.

[7] OJ L 108, 24.4.2002, p. 33.

[8] OJ L 105, 13.4.2006, p. 54."

Declaration by the Netherlands

pursuant to Article 15(3) of Directive 2006/24/EC

Regarding the Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of publicly available electronic communications services and amending Directive 2002/58/EC, the Netherlands will be making use of the option of postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail, for a period not exceeding 18 months following the date of entry into force of the Directive.

Declaration by Austria

pursuant to Article 15(3) of Directive 2006/24/EC

Austria declares that it will be postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail, for a period of 18 months following the date specified in Article 15(1).

Declaration by Estonia

pursuant to Article 15(3) of Directive 2006/24/EC

In accordance with Article 15(3) of the Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Estonia hereby states its intention to make use of use that paragraph and to postpone application of the Directive to retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 36 months after the date of adoption of the Directive.

Declaration by the United Kingdom

pursuant to Article 15(3) of Directive 2006/24/EC

The United Kingdom declares in accordance with Article 15(3) of the Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC that it will postpone application of that Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by the Republic of Cyprus

pursuant to Article 15(3) of Directive 2006/24/EC

The Republic of Cyprus declares that it is postponing application of the Directive in respect of the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until the date fixed in Article 15(3).

Declaration by the Hellenic Republic

pursuant to Article 15(3) of Directive 2006/24/EC

Greece declares that, pursuant to Article 15(3), it will postpone application of this Directive in respect of the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 18 months after expiry of the period provided for in Article 15(1).

Declaration by the Grand Duchy of Luxembourg

pursuant to Article 15(3) of Directive 2006/24/EC

Pursuant to Article 15(3) of the Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, the Government of the Grand Duchy of Luxembourg declares that it intends to make use of Article 15(3) of the Directive in order to have the option of postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by Slovenia

pursuant to Article 15(3) of Directive 2006/24/EC

Slovenia is joining the group of Member States which have made a declaration under Article 15(3) of the Directive of the European Parliament and the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, for the 18 months postponement of the application of the Directive to the retention of communication data relating to Internet, Internet telephony and Internet e-mail.

Declaration by Sweden

pursuant to Article 15(3) of Directive 2006/24/EC

Pursuant to Article 15(3), Sweden wishes to have the option of postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by the Republic of Lithuania

pursuant to Article 15(3) of Directive 2006/24/EC

Pursuant to Article 15(3) of the draft Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC (hereafter the "Directive"), the Republic of Lithuania declares that once the Directive has been adopted it will postpone the application thereof to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for the period provided for in Article 15(3).

Declaration by the Republic of Latvia

pursuant to Article 15(3) of Directive 2006/24/EC

Latvia states in accordance with Article 15(3) of Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC that it is postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 15 March 2009.

Declaration by the Czech Republic

pursuant to Article 15(3) of Directive 2006/24/EC

Pursuant to Article 15(3), the Czech Republic hereby declares that it is postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 36 months after the date of adoption thereof.

Declaration by Belgium

pursuant to Article 15(3) of Directive 2006/24/EC

Belgium declares that, taking up the option available under Article 15(3), it will postpone application of this Directive, for a period of 36 months after its adoption, to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by the Republic of Poland

pursuant to Article 15(3) of Directive 2006/24/EC

Poland hereby declares that it intends to make use of the option provided for under Article 15(3) of the Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of publicly available electronic communications services and amending Directive 2002/58/EC and postpone application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for a period of 18 months following the date specified in Article 15(1).

Declaration by Finland

pursuant to Article 15(3) of Directive 2006/24/EC

Finland declares in accordance with Article 15(3) of the Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC that it will postpone application of that Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by Germany

pursuant to Article 15(3) of Directive 2006/24/EC

Germany reserves the right to postpone application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for a period of 18 months following the date specified in the first sentence of Article 15(1).

Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"

CONTENTS

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

A STRATEGY FOR A SECURE INFORMATION SOCIETY – "DIALOGUE, PARTNERSHIP AND EMPOWERMENT"

1. INTRODUCTION

The Communication "i2010 – A European Information Society for growth and employment"[1], highlighted the importance of network and information security for the creation of a single European information space. The availability, reliability and security of networks and information systems are increasingly central to our economies and to the fabric of society.

The purpose of the present Communication is to revitalise the European Commission strategy set out in 2001 in the Communication "Network and Information Security: proposal for a European Policy approach"[2]. It reviews the current state of threats to the security of the Information Society and determines what additional steps should be taken to improve network and information security (NIS).

Drawing on the experience acquired by Member States and at European Community level, the ambition is to further develop a dynamic, global strategy in Europe, based on a culture of security and founded on dialogue, partnership and empowerment .

In tackling security challenges for the Information Society, the European Community has developed a three-pronged approach embracing: specific network and information security measures, the regulatory framework for electronic communications (which includes privacy and data protection issues), and the fight against cybercrime. Although these three aspects can, to a certain extent, be developed separately, the numerous interdependencies call for a coordinated strategy. This Communication sets out the strategy and provides the framework to carry forward and refine a coherent approach to NIS.

The 2001 Communication defines NIS as " the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems ". Over recent years, the European Community has implemented a number of actions to improve NIS.

The regulatory framework for electronic communications, the review of which is underway, includes security-related provisions. In particular, the Directive on Privacy and Electronic Communications[3] contains an obligation for providers of publicly available electronic communications services to safeguard the security of their services. Provisions against spam[4] and spyware[5] are laid down.

Trust and security also play an important part in the European Community programmes devoted to research and development. The 6th Research Framework Programme addresses these issues through a wide range of projects. Security-related research is to be reinforced in the 7th Framework Programme with the establishment of a European Security Research Programme (ESRP)[6]. Furthermore, the Safer Internet Plus programme supports network-

ing projects and the exchange of best practices to combat harmful content circulating on information networks.

As a part of its response to security threats, the European Community decided in 2004 to create the European Network and Information Security Agency (ENISA). ENISA contributes to the development of a culture of network and information security for the benefit of citizens, consumers, enterprises and public sector organisations throughout the European Union (EU).

The EU also plays an active role in the international fora addressing these topics, such as the OECD, the Council of Europe or the UN. At the World Summit on the Information Society in Tunis, the EU strongly supported the discussions on the availability, reliability and security of networks and information. The Tunis Agenda[7], which together with the Tunis Commitment sets out further steps for the policy debate on the global Information Society as endorsed by the world's leaders, highlights the need to continue the fight against cybercrime and spam while ensuring the protection of privacy and freedom of expression. It identifies the need for a common understanding of the issues of Internet security and for further cooperation to facilitate the collection and dissemination of security-related information and the exchange of good practice among all stakeholders on measures to combat security threats.

2. IMPROVING THE SECURITY OF THE INFORMATION SOCIETY: THE KEY CHALLENGES

Despite the efforts at international, European and national level, security continues to pose challenging problems.

Firstly, attacks on information systems are increasingly motivated by profit rather than by the desire to create disruption for its own sake. Data are illegally mined, increasingly without the user's knowledge, while the number of variants (and the rate of evolution) of malware[8] is increasing rapidly. Spam is a good example of this evolution: it is becoming a vehicle for viruses and fraudulent and criminal activities, such as spyware, phishing[9] and other forms of malware. Its widespread distribution increasingly relies on botnets[10], i.e. compromised servers and PCs used as relays without the knowledge of their owners.

The increasing deployment of mobile devices (including 3G mobile phones, portable videogames, etc.) and mobile-based network services will pose new challenges, as IP-based services develop rapidly. These could eventually prove to be a more common route for attacks than personal computers since the latter already deploy a significant level of security. Indeed, all new forms of communication platforms and information systems inevitably provide new windows of opportunity for malicious attacks.

Another significant development is the advent of "ambient intelligence", in which intelligent devices supported by computing and networking technology will become ubiquitous (e.g. through RFID[11], IPv6 and sensor networks). A totally interconnected and networked everyday life promises significant opportunities. However, it will also create additional security and privacy-related risks. While common platforms and applications contribute positively to interoperability and the take-up of Information and Communication Technologies (ICTs), they can also increase risks. For example, the greater the use of "off-the-shelf" software, the greater the impact when vulnerabilities are exploited or failures occur. The emergence of certain "monocultures" in software platforms and applications can greatly facilitate the growth and spread of security threats such as malware and viruses. Diversity, openness and interoperability are integral components of security and should be promoted .

The relevance of the ICT sector for the European economy and for European society as a whole is incontestable. ICT is a critical component of innovation and is responsible for nearly 40% of productivity growth. In addition, this highly innovative sector is responsible for more than a quarter of the total European R&D effort and plays a key role in the creation of economic growth and jobs throughout the economy. More and more Europeans live in a truly information-based society where the use of ICTs has rapidly accelerated as a core function of human social and economic interaction. According to Eurostat, 89% of EU enterprises actively used the Internet in 2004 and around 50% of consumers had recently used the Internet[12].

A breach in NIS can generate an impact that transcends the economic dimension. Indeed, there is a general concern that security problems may lead to user discouragement and lower take-up of ICT, whereas availability, reliability and security are a prerequisite for guaranteeing fundamental rights on-line.

In addition, because of increased connectivity be-

tween networks, other critical infrastructures (like transport, energy, etc.) are also becoming more and more dependent on the integrity of their respective information systems.

Both business and citizens in Europe still underestimate the risks. This is for various reasons, but the most important seems to be, in the case of enterprises, the poor visibility of the return on investment in security and, in the case of citizens, the fact that they are not aware of their responsibility in the global security chain.

Indeed, given the ubiquity of ICTs and information systems, network and information security is a challenge for everybody:

- Public administrations need to address the security of their systems, not just to protect public sector information, but also to serve as an example of best practice for other players.
- Enterprises need to address NIS more as an asset and an element of competitive advantage than as a "negative cost".
- Individual users need to understand that their home systems are critical for the overall "security chain".

In order to successfully tackle the problems described above, all stakeholders need reliable data on information security incidents and trends. However, reliable and comprehensive data on such incidents are difficult to obtain for many reasons, ranging from the rapidity with which security events can happen to the unwillingness of some organisations to disclose and publicise security breaches. Nonetheless, one of the cornerstones in developing a culture of security is improving our knowledge of the problem.

It is important that awareness programmes, designed to highlight security threats, do not undermine the trust and confidence of consumers and users by focusing only on negative aspects of security. Wherever possible, therefore, NIS should be presented as a virtue and an opportunity rather than as a liability and a cost. It needs to be viewed as an asset in building trust and consumer confidence, a competitive advantage for enterprises operating information systems, and a service quality issue for both public and private sector service providers.

The key challenge for policy makers is to achieve a holistic approach. This approach must recognise the respective roles of the various stakeholders. It must ensure proper coordination of the range of public policy and regulatory provisions that impact either directly or indirectly on NIS. The processes of liberalisation, deregulation and convergence have produced a multiplicity of players among the various stakeholder groups, which does not make this task easier. The contribution of ENISA to this goal can be important. ENISA could serve as a centre for information sharing, cooperation amongst all stakeholders, and the exchange of commendable practices, both within Europe and with the rest of the world, in order to contribute to the competitiveness of our ICT industries and a well-functioning Internal Market.

3. TOWARDS A DYNAMIC APPROACH TO A SECURE INFORMATION SOCIETY

A secure Information Society must be based on enhanced NIS and a widespread culture of security. To this end, the European Commission proposes a dynamic and integrated approach that involves all stakeholders and is based on dialogue, partnership and empowerment. Given the complementary roles of public and private sectors in creating a culture of security, policy initiatives in this field must be based on an open and inclusive multi-stakeholder dialogue.

This approach, and its associated actions, will complement and enrich the Commission's plan to continue the development of a comprehensive and dynamic policy framework through a number of initiatives in 2006:

1. Addressing the evolution of spam and threats, like spyware and other forms of malware, in a Communication on these specific issues.
2. Making proposals for improving cooperation between law enforcement authorities and addressing new forms of criminal activity that exploit the Internet and undermine the operation of critical infrastructures. This will be the subject of a specific Communication on cybercrime.

These policy initiatives also complement the activity being planned to achieve the goals of the Commission's Green Paper on the European Programme for Critical Infrastructure Protection (EPCIP)[13], developed in response to a request by the December 2004 Council. The Green Paper process is likely to lead to an action plan combining an overall "umbrella" approach to critical infrastructure protection with the necessary sector-specific policies, including one for the ICT sector. The sector-specific policy for the ICT sector would examine, via a multi-stakeholder dialogue , the relevant economic, business and societal drivers with a view to enhancing the secu-

rity and the resilience of networks and information systems.

Moreover, the 2006 review of the regulatory framework for electronic communications will also consider elements to improve NIS, such as technical and organisational measures to be taken by service providers, provisions dealing with the notification of security breaches, and specific remedies and penalties regarding breaches of obligations.

It is largely up to the private sector to deliver solutions, services and security products to end users. It is therefore of strategic importance that European industry be both a demanding user of security products and services as well as a competitive supplier of NIS products and services.

National governments need to be able to identify and implement best practice in policy-making, as well as demonstrate commitment to these policy objectives by managing their own information systems in a secure manner. Public authorities, in Member States and at EU level, have a key role to play in properly informing users to enable them to contribute to their own security and safety. Raising awareness on NIS issues and providing appropriate and timely information via dedicated e-security web portals on threats, risks and alerts as well as on best practices should be priorities. To this end, examining the feasibility of creating a European multilingual information sharing and alert system , which would build upon and link together existing or planned national public and private initiatives, could be a major goal for ENISA.

The global dimension of network and information security challenges the Commission, both at international level and in coordination with Member States, to increase its efforts to promote global cooperation on NIS , notably in implementing the agenda adopted at the World Summit on the Information Society (WSIS) in November 2005.

Lastly, research and development, notably at EU level, will help develop new and innovative partnerships to boost the growth of the European ICT industry at large, and the European ICT security industry in particular. The Commission will therefore seek to ensure that appropriate financial resources are allocated to research on NIS and dependability technologies under the 7th EU Framework Programmes.

3.1. Dialogue

3.1.1. As a first step to enhancing dialogue between public authorities, the Commission proposes initiating an exercise to benchmark national NIS-related policies , including specific security policies for the public sector. This exercise will help identify the most effective practices, so that they can then be deployed wherever possible on a broader basis throughout the EU and help make public administrations a driver of best practice in security. The work on electronic identification, for example as part of the recent eGovernment Action Plan, could play an important role in that respect.

If appropriately structured, the results of such a benchmarking exercise will identify best practices to improve awareness among SMEs and citizens of the need to address their own specific NIS challenges and requirements as well as their ability to do so. ENISA should be called upon to play an active role in this dialogue, and in consolidating and exchanging best practices.

3.1.2. A structured multi-stakeholder debate on how best to exploit existing tools and regulatory instruments to attain an appropriate societal balance between security and the protection of fundamental rights, including privacy, is needed. The planned Conference "i2010 – Towards a Ubiquitous European Information Society" being organised by the forthcoming Finnish Presidency, and the consultation on the security and privacy implications of RFID, which is part of the broader consultation recently launched by the Commission, will contribute to this debate. In addition, the Commission will organise:

- A business event to stimulate industry commitment to adopting effective approaches to implement a culture of security in industry.
- A seminar reflecting on ways to raise security awareness and strengthen the trust of end-users in the use of electronic networks and information systems.

3.2. Partnership

3.2.1. Effective policy making needs a clear understanding of the nature and extent of the challenges. This calls for not only reliable and up-to-date statistical and economic data both on information security incidents and levels of consumer and user confidence, but also up-to-date data on the size and trends of the ICT security industry in Europe. The Commission intends to ask ENISA to develop a trusted partnership with Member States and stakeholders to develop an appropriate data collection framework , including the procedures and mechanisms to collect and analyse EU-wide data on secu-

rity incidents and consumer confidence.

In parallel, because of the highly fragmented market in the EU and its rather specific nature, the Commission will invite Member States, the private sector and the research community to establish a strategic partnership to ensure the availability of data on the ICT security industry and on the evolving market trends for products and services in the EU.

3.2.2. In order to improve the European capability to respond to network security threats, the Commission will ask ENISA to examine the feasibility of a European information sharing and alert system to facilitate effective responses to existing and emerging threats to electronic networks. A requirement of such a system will be a multilingual EU portal to provide tailored information on threats, risks and alerts.

3.3. Empowerment

The empowerment of each stakeholder group is a prerequisite to foster awareness of security needs and risks in order to promote NIS.

3.3.1. In this respect the Commission invites Member States to:

- proactively participate in the proposed benchmarking exercise of national NIS policies;
- promote, in close cooperation with ENISA, awareness campaigns on the virtues, benefits and rewards of adopting effective security technologies, practices and behaviour;
- leverage the roll-out of e-government services to communicate and promote good security practices that could then be extended to other sectors;
- stimulate the development of network and information security programmes as part of higher education curricula.

3.3.2. The Commission also invites private sector stakeholders to take initiatives to:

- develop an appropriate definition of responsibilities for software producers and Internet service providers in relation to the provision of adequate and auditable levels of security. Here, support for standardised processes that would meet commonly agreed security standards and best practice rules is needed;
- promote diversity, openness, interoperability, usability and competition as key drivers for security as well as stimulate the deployment of security-enhancing products, processes and services to prevent and fight ID theft and other privacy-intrusive attacks;
- disseminate good security practices for network operators, service providers and SMEs as baseline levels for security and business continuity;
- promote training programmes in the business sector, in particular for SMEs, to provide employees with the knowledge and skills necessary to effectively implement security practices;
- work towards affordable security certification schemes for products, processes and services that will address EU-specific needs (in particular with respect to privacy);
- involve the insurance sector in developing appropriate risk management tools and methods to tackle ICT-related risks and foster a culture of risk management in organisations and business (in particular in SMEs).

4. CONCLUSIONS

Identifying and meeting security challenges in relation to information systems and networks in the EU requires the full commitment of all stakeholders. The policy approach outlined in this Communication seeks to achieve this by reinforcing a multi-stakeholder approach . This would build on mutual interests, identify respective roles and develop a dynamic framework to promote effective public policy-making and private sector initiatives.

The Commission will report to Council and Parliament in the middle of 2007 on the activities launched, the initial findings and the state of play of individual initiatives, including those of ENISA and those taken at Member State level and in the private sector. If appropriate, the Commission will propose a Recommendation on network and information security (NIS).

[1] COM(2005) 229, 1.6.2005.

[2] COM(2001) 298, 6.6.2001.

[3] Directive 2002/58/EC.

[4] Or unsolicited commercial communications.

[5] Spyware is tracking software deployed without adequate notice, consent, or control for the user.

[6] The ESPR is being prepared in the course of a Preparatory Action for Security Research during the period 2004-2006.

[7] Towards a global partnership in the Information Society: follow-up to the Tunis Phase of the World Summit on the Information Society (WSIS) - COM(2006) 181, 27.4.2006.

[8] Malware stands for "malicious software".

[9] Phishing is a form of Internet fraud aiming to steal valuable information such as credit cards, bank account numbers, user IDs and passwords.

[10] Botnets are networks of bots, which are applications that perform actions on behalf of a remote controller and are installed covertly on a victim machine.

[11] Radio Frequency Identification.

[12] Eurostat, Internet activities in the European Union , 40/2005.

[13] COM(2005) 576, 17.11.2005.

Communication from the Commission to the European Parliament, the Council the European Economic and Social Committee and the Committee of the Regions - Communication on the implementation of the multiannual Community Programme on promoting safer use of the Internet and new online technologies (Safer Internet plus)

1. INTRODUCTION

This Communication was drafted in response to a requirement laid down in Article 5(3) of Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual Community programme on promoting safer use of the Internet and new online technologies ("Safer Internet plus"), which states that "the Commission shall report on the implementation of the actions referred to in Article 1(2) to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions by mid-2006 at the latest. In this context, the Commission shall report on the consistency of the amount for 2007 to 2008 with the financial perspective."

The Decision defines the financial framework for the programme as follows (Article 6):

- The financial framework for the period from 1 January 2005 to 31 December 2008 is set at EUR 45 million.
- EUR 20.05 million is provided for the period until 31 December 2006 (Article 6(1)).
- For the period following 31 December 2006, the amount shall be deemed to be confirmed if it is consistent for this phase with the financial perspective in force for the period commencing in 2007 (Article 6(2)).

2. OBJECTIVES OF SAFER INTERNET PLUS

The aim of Safer Internet plus is to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end user.

The Programme focuses on the end-user – particularly children, whether at home or at school.

The Programme is divided into four main actions:

(a) fighting against illegal content;

(b) tackling unwanted and harmful content;

(c) promoting a safer environment;

(d) awareness raising.

Safer Internet plus is a successor to the Safer Internet Action Plan which ran from 1999-2004 with a total budget of EUR 38.3 million.

The coverage of the new programme extends to new online technologies, including mobile and broadband content, online games, peer-to-peer file transfer, and all forms of real-time communications such as chat rooms and instant messages, primarily with the aim of improving the protection of children and minors. A broader range of areas of illegal and harmful content and conduct of concern are covered, including racism and violence.

3. IMPLEMENTATION OF THE PROGRAMME

Safer Internet plus is implemented by the European Commission. The Member States are represented through the Safer Internet plus Management Committee. Financial support is provided through grants and procurements.

3.1. CALL FOR PROPOSALS 2005

In accordance with Article 3 of the programme Decision, the Commission drafted a Work Programme[1] for 2005 to serve as the basis for implementing the programme. The 2005 Safer Internet plus call for proposals was published on 10 September 2005[2].

Following the evaluation, 37 of the 59 proposals received were selected for negotiation, involving indicative EC funding of around EUR 11.79 million in total (of which EUR 9.21 million on the 2005 budget and EUR 2.58 million on the 2006 budget), as follows:

- Hotlines[3]: 1 network coordinator and 16 hotlines covering 15 countries;
- Awareness nodes[4] and helplines[5]: 1 network coordinator and 16 awareness nodes;
- User empowerment: 1 thematic network;
- Self-regulation: 1 thematic network;
- Media: 1 thematic network.

The response to the call was particularly good for the hotlines and the awareness nodes. In fact, the existing hotline network will be extended to the Czech Republic and Slovenia, which did not have hotlines, and the awareness nodes network will be extended to Cyprus, Luxembourg and Latvia, which did not have awareness nodes. Of the 16 awareness nodes recommended for EC funding, 10 will include a helpline as a new service. .

3.2. SAFER INTERNET FORUM

The Safer Internet Forum was set up under the Safer Internet Action Plan to provide a focal point for discussion and encourage action on illegal, unwanted and harmful content. It provides a platform for consensus, inputting conclusions, recommendations, guidelines, etc., to relevant national and European channels. It also provides an opportunity to discuss ways in which industry can contribute to combating illegal content.

In 2005 the main topic discussed in the Safer Internet Forum was "Child safety and mobile phones" focusing on risk assessment, emerging solutions and national codes of conduct[6]. In 2006, discussion with mobile network operators, child safety organisations, researchers and public bodies continued, with the objective of reaching an agreement on best practices on child protection and their implementation across Europe.

In June 2006, two new topics were discussed in the Forum: children's use of new media and blocking access to child sexual abuse images[7].

On the first topic, results of recent research on internet safety were presented. In particular, the Commission presented the results of the last Eurobarometer survey[8], which was launched under a framework contract in December 2005, covering all EU Member States plus Bulgaria, Romania, Croatia and Turkey, to provide comparable data on internet safety issues across Europe.

Earlier surveys were carried out in autumn 2003 in

the 15 "old" Member States and at the beginning of 2004 in the 10 new Member States, just before these countries joined the European Union on 1 May 2004. The new questionnaire was largely based on the 2003/2004 survey to allow comparison. Additional questions were included to better understand the context (parents' use of media) and cover new services (mobile phones, online games, and filtering tools).

According to Eurobarometer, 18% of European parents of children aged 17 and younger say their child has encountered harmful or illegal content on the Internet. Although in the 15 "old" Member States, awareness levels have increased significantly since the previous survey, 44% of parents would like more information about how to protect their child from illegal and harmful content and contact. According to the respondents, this information should be provided by schools (36%), the Internet provider (31%) and the media (21%). Among the recommendations received from stakeholders based on the Eurobarometer results are the following:

- focusing more on children under 10 who are already heavy users of internet and mobile phones;
- improving the visibility of hotlines through enhanced cooperation with the police;
- providing information through channels to suit the needs of the parents and the age of the children (schools, ISPs, media).

The survey also confirmed that internet use, parents' expectations and awareness levels still vary greatly across Europe. Having a European awareness network with national nodes appears to fit in well with running tailored local campaigns.

3.3. SAFER INTERNET DAYS

Safer Internet Day is part of a global drive by awareness-raising partners to promote a safer Internet for all users, especially young people. In February 2005 and 2006, Safer Internet Days were organised under the patronage of Commissioner Viviane Reding by the European internet safety network INSAFE, which is co-funded by the Safer Internet Programme, with the participation of a broad number of organisations and countries across Europe and worldwide.

In 2005, Safer Internet Day was celebrated on 8 February and 65 organisations from 30 countries took part. The event included the launch of a storytelling competition for 9-16 year-olds. Following national ceremonies in 16 countries, a book of their stories has been published.

In 2006, Safer Internet Day was celebrated on 7 February and a broad variety of organisations (around 100 organisations from 37 countries) took part: national authorities, ISPs and telecom operators, industry, schools, libraries and museums, internet safety organisations and international organisations.

Internet safety events such as a worldwide blogathon, quizzes, online games, story-telling competitions, and round table discussions were organised across Europe and also beyond EU borders, for instance in the United States, Russia, Brazil, Argentina, Australia and New Zealand.

More detailed information on the events organised for Safer Internet Day 2006 is available on the programme web site[9].

4. NEW TRENDS FROM 2006

In 2006 the Commission intends to continue the above activities and to enhance their impact by:

- Consolidating and extending the geographical coverage of the hotlines and awareness-raising networks. During the period 2003-2004, under the Safer Internet Action Plan[10], 21 hotlines spanning 20 countries and 23 awareness nodes spanning 21 countries were funded. Most of them will continue operating as a result of the call for proposals for 2005. The new call for proposals for 2006[11] will aim to give the two networks the fullest possible geographical coverage.
- Fostering close cooperation between all stakeholders in Safer Internet activities. This was one of the objectives of the joint annual meeting of hotlines and awareness networks in Luxembourg on 20 June 2006 and the Safer Internet Forum of 21 June 2006, in which researchers, industry, law enforcement authorities and members of the European networks took part.
- Helping European citizens to find practical information about how they can use the Internet more safely. This will be done through the activities of the national awareness nodes and the promotion of a Europe-wide helpline (Europe Direct service)[12].
- Increasing the visibility of the Safer Internet plus programme among European citizens,

both adults and children. In particular, on top of the awareness campaign run by the national awareness nodes, the Commission will organise an event in Brussels for Safer Internet Day 2007.

In implementing Safer Internet plus and in planning a future follow-up programme the Commission will also take account of the findings and recommendations of the final evaluation of the Safer Internet Action Plan[13]. Progress already made in area mentioned by this evaluation will be reinforced.

5.FINANCIAL PERSPECTIVE

Following the interinstitutional agreement on the new financial framework signed on 17 May 2006, the Commission presented its "revised package for EU programmes 2007-2013"[14], amending existing and proposed legislation where necessary to give effect to the agreement. The amount set in this package for Safer Internet plus for the period 2005-2008 is EUR 45 million, exactly the amount provided for in the decision.

The amount set in the programme decision for the period from 1 January 2007 to 31 December 2008 – EUR 24.95 million – is therefore consistent for this phase with the financial perspective in force for the period commencing in 2007.

6.CONCLUSIONS

The great number of reports received by the hotlines (over 534,000 in 2005 alone) shows the increasing need for such a service to fight against illegal content.

Safer Internet Day, with its broad national participation and media coverage, is increasingly recognized as a valuable opportunity to improve communication among stakeholders and to reach out to the broader public.

Awareness nodes are providing more and more targeted campaigns to reach children, parents and teachers and the network is increasingly exchanging best practice in this area.

In order to further build up the actions carried out so far, to achieve the full impact of the programme (e.g. expanding geographical coverage and fostering cooperation among stakeholders), and to enhance its visibility, continued funding is required.

[1] Commission Decision C(2005) 3231 of 9.9.2005, www.europa.eu.int/saferinternet.

[2] OJ C 223, 10.9.2005, p. 8 and Safer internet plus web site:www.europa.eu.int/saferinternet.

[3] Hotlines allow users to report illegal content on the Internet. They pass the reports to the appropriate body (police, ISPs or a correspondant hotline) for action.

[4] Awareness nodes carry out awareness-raising activities aimed at the target groups of parents, teachers and children covering a range of categories of illegal, unwanted and harmful content.

[5] Helplines offer one-to-one conversations with a trained helper (by telephone or online) to allow children to raise concerns about illegal and harmful content on the Internet

[6] http://europa.eu.int/information_society/activities/sip/si_forum/mobile_2005/index_en.htm.

[7] http://europa.eu.int/information_society/activities/sip/si_forum/forum_june_2006/index_en.htm.

[8] http://europa.eu.int/information_society/activities/sip/docs/eurobarometer/eurobarometer_2005_25_ms.pdf.

[9] http://europa.eu.int/information_society/activities/sip/docs/events/si_day_2006_events.pdf.

[10] Decision no 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (OJ L 33 of 6.2.1999 p.1) amended by Decision no 1151/2003/EC of the European Parliament and of the Council of 16 June 2003 (OJ L 162 of 1.7.2003).

[11] OJ C167 of 19.7.2006 and Safer Internet plus web site: http://europa.eu.int/information_society/activities/sip/call/proposals/index_en.htm.

[12] http://europa.eu/europedirect and free-number 00800 6 7 8 9 10 11.

[13] COM/2006/XXXX of ….

[14] IP/06/673 of 24/05/2006 and MEMO/06/213.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on fighting spam, spyware and malicious software

1. PURPOSE OF THE COMMUNICATION

Society is becoming more and more aware of how essential modern electronic communications networks and services are for everyday life, in business or at home. A wide take-up of services depends on trustworthy, secure and reliable technologies. The Commission Communication on a Strategy for a secure Information Society [1] aims at improving the security of network and information at large and invites the private sector to address vulnerabilities in network and information systems that can be exploited to spread spam and malicious software. The Commission Communication on the Review of the EU Regulatory Framework proposes new rules to strengthen security and privacy in the electronic communications sector [2].

The present Communication deals with the evolution of spam [3], and threats such as spyware and malicious software. It takes stock of efforts made so far to fight these threats and identifies further actions that can be taken, including:

- strengthening Community law
- law enforcement
- cooperation within and between Member States
- political and economic dialogue with third countries
- industry initiatives
- R&D activities.

2. THE PROBLEM - THE EVOLVING NATURE OF THREATS

Spam [4] has grown significantly over the last 5 years [5]. Industry sources report that spam now accounts for 50-80% of messages addressed to end-users. [6]. Although the biggest portion of spam originates from outside the EU, European countries now account for 25% of relayed spam messages [7]. The worldwide cost of spam has been estimated at €39 billion in 2005. Spam costs to major European economies have been estimated to be around respectively €3,5 billion – Germany, €1,9 billion –United Kingdom and €1,4 billion - France [8]. Spamming is considered a 'business' of its own. Spammers rent or sell lists of harvested e-mail addresses to companies for marketing purposes. Spam over the internet is especially lucrative. This has to do with the reach of the medium and the low costs involved in sending massive amounts of messages. At the same time moderate investments to fight spam can also deliver significant results. As an example, in the Netherlands an 85% reduction in Dutch spam was achieved by investing €570 000 in equipment to fight spam.

From a mere nuisance unsolicited e-mail has become increasingly fraudulent and criminal in nature. A prominent example is the use of phishing e-mails that lure end users into giving up sensitive data via imitation websites purporting to represent genuine companies, raising concerns about possible identity fraud and damage to companies' reputations. The dissemination of spyware by e-mail or through software to track and report a user's on-line behaviour continues to increase. Spyware may also collect personal information such as passwords and credit card numbers.

The sending of massive amounts of unsolicited e-mail is greatly facilitated by the spread of malicious codes such as worms and viruses. Once installed, they allow an attacker to take over control of an infected computer system and turn it into a 'botnet', [9] hiding the identity of the real spammer. Botnets are hired by spammers, phishers, and spyware vendors for fraudulent and criminal purposes. Industry experts estimate that 'botnets' relay over 50 percent of abusive e-mails [10]. The spread of spyware and other types of malicious codes attacking consumers and businesses has a considerable economic impact. The global financial impact of malware has been estimated about €11 billion in 2005 [11].

3. THE WORK DONE SO FAR - ACTIONS UNDERTAKEN SINCE 2004

The EU adopted in 2002 a Directive on Privacy and Electronic Communications that puts a ban on spam [12] by introducing the principle of consent-based marketing to natural persons. In January 2004, the Commission presented a Communication on

spam identifying actions to complement the Directive [13]. The Communication stressed the need for action by various actors in the areas of awareness, self-regulation/technical actions, cooperation and enforcement. The Commission has started to include the issue of the fight against spam, spyware and malware in its dialogue with third countries. In addition, the Unfair Commercial Practices Directive [14] protects consumers against aggressive commercial practices; cross border cooperation to fight such practices comes under the Regulation on Consumer Protection Cooperation [15].

3.1. Awareness actions

The Commission Communication contributed in raising awareness of spam at national and international level around the globe. At EU level, the Safer Internet plus programme promotes safer use of the Internet and new online technologies, particularly for children, as part of a coherent approach by the European Union.

Member States have launched or supported campaigns to make users aware of the spam problem and how to deal with it. Generally ISPs have taken responsibility in providing their customers with advice and assistance on how to protect themselves against spyware and viruses. The Commission hosted an OECD workshop on spam in February 2004. The Commission also contributed actively to the OECD Anti-Spam Toolkit that provides a comprehensive package of regulatory approaches, technical solutions, and industry initiatives to fight spam.

The UN World Summit on the Information Society [16] recognised that spam should be dealt with at appropriate national and international levels. WSIS thematic conferences have been held by the ITU in 2004 and 2005. The WSIS Tunis Agenda adopted in November 2005 calls to deal effectively with the significant and growing problem posed by spam [17].

3.2. International Cooperation

Spam is a cross-border issue, and several cooperation initiatives and cross-border enforcement mechanisms have been put in place. The Commission has set up a Contact Network of Spam Authorities (CNSA), which meets regularly, exchanges best practices and cooperates on enforcement across borders. The CNSA has drawn up a cooperation procedure [18] to facilitate cross-border handling of spam complaints. The Commission services support and participate as observers in the London Action Plan, which gathers enforcement authorities from 20 countries and has also adopted a cross border cooperation procedure. A joint EU CNSA – LAP workshop was held in November 2005. The OECD adopted a Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam which was adopted in April 2006, urging enforcement authorities to share information and work together [19].

The Commission is further promoting international cooperation initiatives. The US and the EU have agreed 'to cooperate to tackle spam through joint enforcement initiatives, and explore ways to fight against illegal "spyware" and "malware". The Commission also takes part in the Canadian International Collaboration working group on Spam. Discussions are taking place with major international partners e.g., China, Japan. Concerning Asia the Commission initiated a Joint Statement on International Antispam Cooperation which was adopted at the ASEM conference on eCommerce in February 2005 [20].

The Tunis Agenda, adopted by the World Summit of Information Society in November 2005, stresses that internet security is an area where a better international cooperation is needed and that this issue will need to be addressed in the framework of the enhanced cooperation model for internet governance that will be implemented as a follow-up of the Summit. [21].

3.3. Research and Technology development

Under the 6th RTD Framework Program, the Commission has launched projects to help stakeholders fight spam and other forms of malware. These projects [22] range from general network monitoring and detection of attacks to the specific development of technologies to build filters to detect spam, phishing and malware. Achievements include the establishment of a research community dedicated to malware containment and the development of a European infrastructure to monitor Internet traffic. Recently-started activities concern adaptive phishing filters which can detect unknown threats, and cyber attacks. The financial effort dedicated to these activities amounts to €13.5 million.

3.4. Industry actions

The Commission welcomes industry's pro-active role in relation to spam. Service providers in general have taken technical measures to tackle spam, including better spam filters. ISPs have set up help desk support and provide users with software against spam, spyware and malware. Many ISPs have contractual clauses in place that forbid on-line mal-

practices. In a recent civil UK court case a €68 800 fine was imposed on a spammer for breach of contract. Industry groups have adopted best practices to prevent on-line phishing and to improve filtering methods [23].

Mobile operators have acted Industry codes of conduct foresee taking action against unsolicited messages. The GMSA has published a Code of practice on Mobile spam in 2006. Currently the Commission co-funds the Spotspam initiative – a partnership between private and public bodies which aims to build a database to facilitate the cross border investigation and enforcement of spam cases [24].

3.5. Enforcement actions

It is clear that taking up the fight against spam delivers results. Filtering measures imposed in Finland reduced the proportion of spam in the transmitted e-mail from 80 % to about 30 %. A large number of authorities have undertaken enforcement efforts to stop spammers [25].

There are however significant differences between Member States in the actual number of prosecuted cases. Some authorities have launched a hundred or more investigations that have led to successfully ending and penalising spam activities. In other Member States the number of cases investigated has not been more than a handful or in some cases zero.

Most actions have been targeted at 'traditional' forms of spam; other noted threats have hardly been prosecuted even though they create major risks.

4. THE WAY FORWARD: WORK TO BE DONE

4.1. Action at Member States level

This section covers actions targeted at Governments and national authorities in particular related to enforcement and cooperation.

4.1.1. Critical success factors

The persistency and evolving nature of the problem calls for greater involvement and prioritisation by Member States. Actions should in particular address 'professional' spammers, phishers and the spreading of spyware and malware. Critical success factors are:

- A strong commitment by central government to fight on-line malpractices
- Clear organisational responsibility for enforcement activities
- Adequate resources for the enforcement authority.

Currently, these factors are not present in all Member States.

4.1.2. Coordination and integration at national level

Under the e-Privacy Directive and the General Data Protection Directive [26], national authorities have the power to act against the following illegal practices:

- sending unsolicited communications (spam) [27];
- unlawful access to terminal equipment; either to store information -such as adware and spyware programs- or to access information stored on that equipment [28];
- infecting terminal equipment by inserting malware such as worms and viruses and turning PCs into botnets or usage for other purposes [29];
- misleading users into giving away sensitive information [30] such as passwords and credit card details by so called phishing messages.

Some of these practices also fall under criminal law, including the Framework Decision on attacks against information systems [31]. According to the latter, Member States have to provide for a maximum penalty of at least 3 years imprisonment, or 5 years if committed by organised crime.

At a national level, these provisions may be enforced by administrative bodies and/or criminal law authorities. Where this is the case, the responsibilities of different authorities and cooperation procedures need to be clearly spelled out. This may require decisions being taken at a high level in national governments.

To date, the increasingly entwined criminal and administrative aspects of spam and other threats have not been reflected in a corresponding growth of cooperation procedures in Member States that brings together the technical and investigative skills of different agencies. Cooperation protocols are needed to cover such areas as exchange of information and intelligence, contact details, assistance, and transfer of cases.

Close cooperation between enforcement authorities, network operators and ISPs at national level is also beneficial for exchange of information, technical expertise and the pursuit of on-line malpractices. Authorities from Norway and the Netherlands have reported on the usefulness of such public-private partnerships.

4.1.3. Resources

Resources are needed to gather evidence, pursue investigations, and mount prosecutions. Authorities need technical and legal resources and must acquaint themselves with the way offenders operate to successfully put their practices to an end.

On-line complaint mechanisms, with associated systems to log and analyse reported malpractices, can be an important tool. Experience has shown that moderate investments can bring significant results. The reduction in Dutch spam was achieved by establishing a team of 5 full time dedicated employees in OPTA, the Dutch authority, with €570 000 in equipment to fight spam. Building on this investment, the experience gained in fighting spam is now being used to target other problem areas.

4.1.4. Cross border cooperation

Spam is a global problem. National authorities will often have to rely on authorities in other countries to prosecute spammers, and conversely, may be called upon to pursue investigations coming from other countries.

While there may be some reluctance to commit scarce national resources to investigate other people's problems, it is important for Member States to recognise that effective cross-border cooperation is an essential element in fighting spam. Recently the Australian and Dutch spam fighting authorities cooperated in bringing down a large spam operation.

To date 21 European authorities have endorsed the CNSA cooperation procedure [32] on cross border complaint handling; the remaining authorities are invited to do likewise within the next few months. Member States and competent authorities are in particular invited to actively promote the use of:

- the Joint CNSA-LAP pro forma documents
- the OECD Recommendation and Toolkit on spam enforcement.

4.1.5 Proposed actions

Member States and competent authorities are called upon to:

- lay down clear lines of responsibility for national agencies involved in fighting spam
- ensure effective coordination between competent authorities
- involve market players at national level, drawing on their expertise and available information
- ensure that adequate resources are made available to enforcement efforts
- subscribe to international cooperation procedures and act on requests for cross border assistance

4.2. Action by industry

This section covers actions that can be taken by industry to promote consumer trust and mitigate the sending of abusive e-mails.

4.2.1. Software delivery and installation

Spyware poses a serious threat to users' privacy. On-line software offerings have become a much employed method for delivery and installation of spyware on user's terminal equipment. Spyware can also be hidden in software distributed through other media such as CD-ROMs for installation on a computer. Unwanted spying programmes may be installed together with the software that the consumer acquires.

To prevent spyware from reaching end-users specific actions are identified below.

4.2.2. Informing the consumer

Software offers may include the installation of additional programmes. Where this added software operates as spyware by monitoring end-users behaviour (e.g. for marketing purposes) this involves the processing of personal data, and is illegal without the user's informed consent. In many cases, the user's consent to install such software is either not obtained or else is hidden in the small print of a long end-user licence agreement.

Companies that offer software products are encouraged to clearly and prominently describe all the terms and conditions of the offer, in particular if

there is processing of personal data by any monitoring devices that are included in software packages.

Self regulation and the use of some sort of 'seal of approval' could provide a means to separate trustworthy companies from those who are not. Codes of conduct, which aim to inform the user on conditions that imply the processing of personal data, can be submitted for endorsement to the Article 29 Data Protection Working Party.

4.2.3 Contract clauses in the chain of supply

Often companies are not aware of how advertisements of their products and services are technically being delivered to the public. Legitimate software may be packaged with spyware used to gain access to sensitive data, including credit card data, confidential documents etc.

Companies that advertise and or sell products need to ensure that their contracting parties' activities are legitimate. A company needs to understand the contracting chain of relationships, monitor legal compliance and make malpractice subject to termination throughout the chain, so that further affiliation with mal-practicing companies can be ended immediately.

4.2.4. Security measures by service providers

An ENISA survey in 2006 [33] confirms that service providers in general have taken measures to tackle spam. It does however report that service providers could further contribute to the overall security of the network, and recommends that more emphasis is put on filtering e-mail that leaves a service providers network (egress filtering). The Commission encourages service providers to implement this recommendation.

The Article 29 Data Protection Working Party adopted an Opinion on privacy issues related to the provision of email screening services [34] which provides guidance on the question of confidentiality of email communications and, more specifically, on the filtering of on-line communications against viruses, spam, and illegal content.

4.2.5. Proposed actions

The Commission invites:

- companies to ensure that the standard of information for the purchase of software applications is in accordance with data protection law.
- companies to contractually prohibit illegal use of software in advertisements, monitor how advertisements reach consumers and follow up on malpractice.
- e-mail service providers to apply a filtering policy which ensures compliance with the recommendation and guidance on e-mail filtering.

4.3. Action at European level

The Commission will continue to address the issues surrounding spam, spyware and malware in international fora, in bilateral meetings and where appropriate through agreements with third countries and will continue to foster cooperation between stakeholders including Member States, competent authorities and industry. It will also take new initiatives in the area of legislation and research that aim to provide fresh impetus in the fight against malpractices that undermine the Information Society. The Commission is currently working on the further development of a coherent policy on the fight against cyber crime. This policy will be presented in a Communication planned for adoption in the beginning of 2007.

4.3.1. Review of the regulatory framework

The Commission Communication [35] on the regulatory framework for electronic communications proposes to strengthen the rules in the area of privacy and security. Under the proposal, network operators and service provider would be obliged to:

- notify the competent authority in a Member State of any breach of security that led to the loss of personal data and/or to interruptions in the continuity of service supply.
- notify their customers of any breach of security leading to the loss, modification, access or destruction of personal customer data.

National regulatory authorities would have the power to ensure operators implement adequate security policies and new rules could be established providing for specific remedies or an indication of the level of penalties to be expected for breaches.

4.3.2. Role of ENISA

The proposals also include a provision recognising the advisory role of ENISA in security matters. Other tasks foreseen for ENISA are outlined in the Commis-

sion Communication on a Security Strategy [36] and include:

- to build a trusted partnership with Member States and stakeholders to develop an appropriate data collection framework on security incidents and levels of consumer confidence.

ENISA will closely coordinate that Framework with Eurostat in view of the Community statistics concerning the information society and the i2010 benchmarking framework [37].

- to examine the feasibility of a European information sharing and alert system to facilitate effective responses to existing and emerging threats to electronic networks.

4.3.3. Research and development

The forthcoming FP7 program aims at the continued development of knowledge and technologies to secure information services and systems in close coordination with policy initiatives. Topics of work related to malware are expected to include hidden botnets and viruses, and attacks on mobile and voice services.

4.3.4. International cooperation

As the internet is a global network, the commitment to fight spam, spyware and malware needs to be shared around the world. Hence, the Commission intends to reinforce the dialogue and the cooperation with third countries on the fight against these threats and criminal activities that are linked to them. To this end, , the Commission will seek to ensure that spam, spyware and malware is addressed in agreements between the EU and third countries, will seek firm commitment of the most concerned third countries to work with EU member states to fight these threats more effectively, and will closely follow-up the enforcement of jointly committed objectives.

4.3.5. Proposed actions

The Commission will:

- continue efforts in raising awareness and fostering cooperation between stakeholders
- continue to develop agreements with third countries including the issue of the fight against spam, spyware and malware
- aim to introduce new legislative proposals at the beginning of 2007 that strengthen the rules in the area of privacy and security in the communications sector and present a policy on cyber crime
- involve ENISA expertise in security matters
- support research and development in its FP7 program.

5. CONCLUSION

Threats such as spam, spyware and malware undermine the confidence in, and the security of, the Information Society, and have a significant financial impact. While some Member States have taken initiatives, over the EU as a whole there is insufficient action to address this development. The Commission is using its role as an intermediary to create greater awareness about the need for greater political commitment to fight these threats.

Enforcement efforts need to be stepped up to stop those who knowingly disobey the law. Further action by industry should be undertaken to complement enforcement activities. Cooperation is needed at national level both within government and between government and industry. The Commission will reinforce the dialogue and the cooperation with third countries and also examine the opportunity to make new legislative proposals and will undertake research actions to further strengthen privacy and security in the electronic communication sector.

Integrated and, where possible, parallel implementation of the actions identified in this Communication can contribute to reducing the threats that are currently compromising the benefits of the Information Society and the economy.

The Commission will monitor the implementation of these actions and assess by 2008 whether additional action is needed.

[1] COM(2006) 251 final

[2] COM(2006) 334 final.

[3] COM(2004) 28 final

[4] Spam refers to sending unsolicited communications –e.g. by e-mail- for commercial purposes. However, unsolicited e-mail messages may also carry malicious software and spyware.

[5] In 2001 spam was 7% of global e-mail traffic.

[6] Symantec 54%; Messagelabs 68,6 MAAWG 80-85.

[7] Q1 2006 (Sophos) Asia 42.8%, N. America 25.6, Europe 25.0, S. America, 5.1, Australasia 0.8 Africa 0.6, Other 0.1.

[8] Ferris research, 2005.

[9] Botnets are compromised computers used by spammers to send bulk e-mails by installing hidden software that turns computers into mail servers without the users' knowledge.

[10] Symantec top botnet infected countries, (Q 3-4 2005) : US 26 %, U K 22%, China 9%, France, S. Korea, Canada 4%, Taiwan, Spain, Germany 3%,Japan 2%.

[11] Computer Economics: the 2005 Malware Report.

[12] Art. 13 Directive 2002/58.

[13] Supra 3.

[14] Annex 1, point 26, Directive 2005/29/EC

[15] Regulation (EC) 2006/2004

[16] WSIS, Geneva, December 2003.

[17] Tunis Agenda, para. 41.

[18] http://europa.eu.int/information_society/policy/ecomm/doc/todays_framework/privacy_protection/spam/cooperation_procedure_cnsa_final_version_20041201.pdf

[19] http://www.oecd-antispam.org/

[20] http://www.asemec-london.org/

[21] Tunis Agenda para's 39-47. http://www.itu.int/wsis/docs2/tunis/off/6rev1.doc

[22] www.diademhttp://cordis.europa.eu/fp6/projects.htm#search

[23] http://www.maawg.org/home/

[24] http://www.spotspam.net

[25] A CNSA survey showed that fifteen out of eighteen responding members prosecuted cases in the period 2003-2006.

[26] Directive 95/46/EC.

[27] Art. 13 e-Privacy Directive.

[28] Art. 5 (3) e-Privacy Directive.

[29] Supra 28.

[30] Art. 6 (a) General Data Protection Directive.

[31] Council Framework Decision 2005/222/JHA.

[32] Supra 18.

[33] http://www.enisa.eu.int/doc/pdf/deliverables/enisa_security_spam.pdf

[34] Opinion 2/2006, WP 118.

[35] http://europa.eu.int/information_society/policy/ecomm/tomorrow/index_en.htm

[36] Supra 1.

[37] I2010 High Level Group benchmarking framework of 20 April 2006.

Communication from the Commission on a European Programme for Critical Infrastructure Protection

1. BACKGROUND

The European Council of June 2004 asked for the preparation of an overall strategy to protect critical infrastructure. The Commission adopted on 20 October 2004 a Communication on Critical Infrastructure Protection in the Fight against Terrorism which put forward suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving Critical Infrastructures (CI).

The Council conclusions on "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks" adopted by Council in December 2004 endorsed the intention of the Commission to propose a European Programme for Critical Infrastructure Protection (EPCIP) and agreed to the setting up by the Commission of a Critical Infrastructure Warning Information Network (CIWIN).

In November 2005, the Commission adopted a Green Paper on a European Programme for Critical Infrastructure Protection (EPCIP) which provided policy options on how the Commission could establish EPCIP and CIWIN.

The 2005 December Justice and Home Affairs (JHA) Council Conclusions on Critical Infrastructure Protection called upon the Commission to make a proposal for a European Programme for Critical Infrastructure Protection.

This Communication sets out the principles, processes and instruments proposed to implement EPCIP. The implementation of EPCIP will be supplemented where relevant by sector specific Communications setting out the Commission's approach concerning particular critical infrastructure sectors[1].

2. PURPOSE, PRINCIPLES AND CONTENT OF EPCIP

2.1. The objective of EPCIP

The general objective of EPCIP is to improve the protection of critical infrastructures in the EU. This objective will be achieved by the creation of an EU framework concerning the protection of critical infrastructures which is set out in this Communication.

2.2. Types of threats to be addressed by EPCIP

While recognising the threat from terrorism as a priority, the protection of critical infrastructure will be based on an all-hazards approach. If the level of protective measures in a particular CI sector is found to be adequate, stakeholders should concentrate their efforts on threats to which they are vulnerable.

2.3. Principles

The following key principles will guide the implementation of EPCIP:

- Subsidiarity – The Commission's efforts in the CIP field will focus on infrastructure that is critical from a European, rather than a national or regional perspective. Although focusing on European Critical Infrastructures, the Commission may where requested and taking due account of existing Community competences and available resources provide support to Member States concerning National Critical Infrastructures.
- Complementarity - the Commission will avoid duplicating existing efforts, whether at EU, national or regional level, where these have proven to be effective in protecting critical infrastructure. EPCIP will therefore complement and build on existing sectoral measures.
- Confidentiality - Both at EU level and MS level, Critical Infrastructure Protection Information (CIPI) will be classified appropriately and access granted only on a need-to-know basis. Information sharing regarding CI will take place in an environment of trust and security.
- Stakeholder Cooperation – All relevant stakeholders will, as far as possible, be involved in the development and implementation of EPCIP. This will include the owners/operators of critical infrastructures designated as ECI as well as public authorities and other relevant bodies.
- Proportionality – measures will only be proposed where a need has been identified following an analysis of existing security gaps and will be proportionate to the level of risk and type of threat involved.
- Sector-by-sector approach – Since various sectors possess particular experience, expertise and requirements with CIP, EPCIP will be developed on a sector-by-sector basis and implemented following an agreed list of CIP sectors.

2.4. The EPCIP framework

The framework will consist of:

- A procedure for the identification and designation of European Critical Infrastructures (ECI), and a common approach to the assessment of the needs to improve the protection of such infrastructures. This will be implemented by way of a Directive.
- Measures designed to facilitate the implementation of EPCIP including an EPCIP Action Plan, the Critical Infrastructure Warning Information Network (CIWIN), the use of CIP expert groups at EU level, CIP information sharing processes and the identification and analysis of interdependencies.
- Support for Member States concerning National Critical Infrastructures (NCI) which may optionally be used by a particular Member State. A basic approach to protecting NCI is set out in this Communication.
- Contingency planning.
- An external dimension.
- Accompanying financial measures and in particular the proposed EU programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013, which will provide funding opportunities for CIP related measures having a potential for EU transferability.

Each of these measures is addressed below.

2.5. The CIP Contact Group

An EU level mechanism is required in order to serve as the strategic coordination and cooperation platform capable of taking forward work on the general aspects of EPCIP and sector specific actions. Conse-

quently, a CIP Contact Group will be created.

The CIP Contact Group will bring together the CIP Contact Points from each Member State and will be chaired by the Commission. Each Member State should appoint a CIP Contact Point who would coordinate CIP issues within the Member State and with other Member States, the Council and the Commission. The appointment of the CIP Contact Point would not preclude other authorities in the Member State from being involved in CIP issues.

3. EUROPEAN CRITICAL INFRASTRUCTURES (ECI)

European Critical Infrastructures constitute those designated critical infrastructures which are of the highest importance for the Community and which if disrupted or destroyed would affect two or more MS, or a single Member State if the critical infrastructure is located in another Member State. This includes transboundary effects resulting from interdependencies between interconnected infrastructures across various sectors. The procedure for the identification and designation of European Critical Infrastructures (ECI), and a common approach to the assessment of the needs to improve the protection of such infrastructures will be established by means of a Directive.

4. MEASURES DESIGNED TO FACILITATE THE DEVELOPMENT AND IMPLEMENTATION OF EPCIP

A number of measures will be used by the Commission to facilitate the implementation of EPCIP and to further EU level work on CIP.

4.1. EPCIP Action Plan

EPCIP will be an ongoing process and regular review will be carried out in the form of the EPCIP Action Plan (Annex). The Action Plan will set out the actions to be achieved along with relevant deadlines. The Action Plan will be updated regularly based on the progress made.

The EPCIP Action Plan organizes CIP related activities around three work streams:

- Work Stream 1 which will deal with the strategic aspects of EPCIP and the development of measures horizontally applicable to all CIP work.
- Work Stream 2 dealing with European Critical Infrastructures and implemented at a sectoral level.
- Work Stream 3 which will support the Member States in their activities concerning National Critical Infrastructures.

The EPCIP Action Plan will be implemented taking into account sector specificities and involving, as appropriate, other stakeholders.

4.2. Critical Infrastructure Warning Information Network (CIWIN)

The Critical Infrastructure Warning Information Network (CIWIN) will be set up through a separate Commission proposal and due care will be taken to avoid duplication. It will provide a platform for the exchange of best practices in a secure manner. CIWIN will complement existing networks and could also provide an optional platform for the exchange of rapid alerts linked to the Commission's ARGUS system. The necessary security accreditation of the system will be undertaken in line with relevant procedures.

4.3. Expert groups

Stakeholder dialogue is crucial for improving the protection of critical infrastructures in the EU. Where specific expertise is needed the Commission may therefore setup CIP expert groups at EU level to address clearly defined issues and to facilitate public-private dialogue concerning critical infrastructure protection. Expert groups will support EPCIP by facilitating exchanges of views on related CIP issues on an advisory basis. These expert groups constitute a voluntary mechanism in which public and private resources are blended to achieve a goal or set of goals judged to be of mutual benefit both to citizens and the private sector.

CIP expert groups will not replace other existing groups already established or which could be adapted to fulfil the needs of EPCIP, nor will they interfere with direct information exchanges between industry, the MS authorities and the Commission.

An EU level CIP expert group will have a clearly stated objective, a timeframe for the objective to be achieved and clearly identified membership. CIP Expert Groups will be dissolved following the achievement of their objectives.

Specific functions of CIP expert groups may vary across CI sectors depending on the unique characteristics of each sector. These functions may include

the following tasks:

- Assist in identifying vulnerabilities, interdependencies and sectoral best practices;
- Assist in the development of measures to reduce and/or eliminate significant vulnerabilities and the development of performance metrics;
- Facilitating CIP information-sharing, training and building trust;
- Develop and promote "business cases" to demonstrate to sector peers the value of participation in infrastructure protection plans and initiatives;
- Provide sector-specific expertise and advice on subjects such as research and development.

4.4. The CIP information sharing process

The CIP information sharing process among relevant stakeholders requires a relationship of trust, such that the proprietary, sensitive or personal information that has been shared voluntarily will not be publicly disclosed and that that sensitive data is adequately protected. Care must be taken to respect privacy rights.

Stakeholders will take appropriate measures to protect information concerning such issues as the security of critical infrastructures and protected systems, interdependency studies and CIP related vulnerability, threat and risks assessments. Such information will not be used other than for the purpose of protecting critical infrastructure. Any personnel handling classified information will have an appropriate level of security vetting by the Member State of which the person concerned is a national.

In addition, CIP information exchange will recognize that certain CIP information, though unclassified, may still be sensitive and therefore needs to be treated with care.

CIP information exchange will facilitate the following:

- Improved and accurate information and understanding about interdependencies, threats, vulnerabilities, security incidents, countermeasures and best practices for the protection of CI;
- Increased awareness of CI issues;
- Stakeholder dialogue;
- Better-focused training, research and development.

4.5. Identification of interdependencies

The identification and analysis of interdependencies, both geographic and sectoral in nature, will be an important element of improving critical infrastructure protection in the EU. This ongoing process will feed into the assessment of vulnerabilities, threats and risks concerning critical infrastructures in the EU.

5. NATIONAL CRITICAL INFRASTRUCTURES (NCI)

With due regard to existing Community competences, the responsibility for protecting National Critical Infrastructures falls on the NCI owners/operators and on the Member States. The Commission will support the Member States in these efforts where requested to do so.

With a view to improving the protection of National Critical Infrastructures each Member State is encouraged to establish a National CIP Programme. The objective of such programmes would be to set out each Member State's approach to the protection of National Critical Infrastructures located within its territory. Such programmes would at a minimum address the following issues:

- The identification and designation by the Member State of National Critical Infrastructures according to predefined national criteria. These criteria would be developed by each Member State taking into account as a minimum the following qualitative and quantitative effects of the disruption or destruction of a particular infrastructure:
- Scope - The disruption or destruction of a particular critical infrastructure will be rated by the extent of the geographic area which could be affected by its loss or unavailability.
- Severity - The consequences of the disruption or destruction of a particular infrastructure will be assessed on the basis of:
- Public effect (number of population affected);
- Economic effect (significance of economic loss and/or degradation of products or services);

- Environmental effect;
- Political effects;
- Psychological effects;
- Public health consequences.

Where such criteria do not exist, the Commission will assist a Member State, at its request, in their development by providing relevant methodologies.

- The establishment of a dialogue with CIP owners/operators.
- Identification of geographic and sectoral interdependencies.
- Drawing-up NCI related contingency plans where deemed relevant.
- Each Member State is encouraged to base its National CIP Programme on the common list of CI sectors established for ECI.

The introduction of similar approaches to the protection of NCI in the Member States would contribute to ensuring that CI stakeholders throughout Europe benefit from not being subjected to varying frameworks resulting in additional costs and that the Internal Market is not distorted.

6. CONTINGENCY PLANNING

CONTINGENCY PLANNING IS A KEY ELEMENT OF THE CIP PROCESS SO AS TO MINIMIZE THE POTENTIAL EFFECTS OF A DISRUPTION OR DESTRUCTION OF A CRITICAL INFRASTRUCTURE. THE DEVELOPMENT OF A COHERENT APPROACH TO THE ELABORATION OF CONTINGENCY PLANS ADDRESSING SUCH ISSUES AS THE PARTICIPATION OF OWNERS/OPERATORS OF CRITICAL INFRASTRUCTURE, COOPERATION WITH NATIONAL AUTHORITIES AND INFORMATION SHARING AMONG NEIGHBOURING COUNTRIES SHOULD FORM AN IMPORTANT ELEMENT OF THE IMPLEMENTATION OF THE EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION.

7. EXTERNAL DIMENSION

Terrorism, other criminal activities, natural hazards and other causes of accidents are not constrained by international borders. Threats cannot be seen in a purely national context. Consequently, the external dimension of Critical Infrastructure Protection needs to be fully taken in to account in the implementation of EPCIP. The interconnected and interdependent nature of today's economy and society means that even a disruption outside of the EU's borders may have a serious impact on the Community and its Member States. Equally true, the disruption or destruction of a critical infrastructure within the EU may have a detrimental effect on the EU's partners. Finally, working toward the goal of increasing the protection of critical infrastructure within the EU will minimize the risk of the EU economy being disrupted and thereby contribute to the EU's global economic competitiveness.

Consequently, enhancing CIP cooperation beyond the EU through such measures as sector specific memoranda of understanding (e.g. on the development of common standards, undertaking joint CIP related studies, identification of common types of threats and exchanging best-practices on protection measures) and encouraging the raising of CIP standards outside of the EU should therefore be an important element of EPCIP. External cooperation on CIP will primarily focus on the EU's neighbours. Given however the global interconnectedness of certain sectors including ICT and financial markets, a more global approach would be warranted. Dialogue and the exchange of best practices should nevertheless involve all relevant EU partners and international organizations. The Commission will also continue promoting improvements in the protection of critical infrastructures in non-EU countries by working with G8, Euromed and European Neighbourhood Policy partners through existing structures and policies, including the "Instrument for Stability".

8. ACCOMPANYING FINANCIAL MEASURES

The Community programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013 will contribute to the implementation of EPCIP.

Within the general objectives, and unless covered by other financial instruments, the programme will stimulate, promote and develop measures on prevention, preparedness and consequence management aimed at preventing or reducing all security risks, in particular risks linked with terrorism, where appropriate based on comprehensive threat and risk assessments.

Funding under the programme, by way of grants and Commission initiated actions, will be used in particular toward the development of instruments, strategies, methodologies, studies, assessments and activities/measures in the field of the effective pro-

tection of critical infrastructure (at both EU and MS levels).

ANNEX

EPCIP Action Plan

Work Stream 1. Consecutive EPCIP strategies

Work stream 1 will serve as the strategic platform for overall EPCIP coordination and cooperation through the EU CIP Contact Group.

Phase 1

Action | Actor | Timeframe |

Identification of priority sectors for action (The transport and energy sectors will be among the first priorities) | Commission | As soon as possible and thereafter on an annual basis |

Development of common CI sector-based working definitions and terminology | Commission, MS and other stakeholders where relevant | at the latest one year following the entry into force of the ECI Directive |

Elaboration of general criteria to be used in identifying ECI | Commission, MS and other stakeholders where relevant | at the latest one year following the entry into force of the ECI Directive |

Creation of an inventory of existing national, bilateral and EU critical infrastructure protection programmes | Commission, MS | ongoing |

Creation and agreement on guidelines on collection and use of sensitive data between stakeholders | Commission, MS, and other stakeholders where relevant | ongoing |

Collection of CIP related best practices, risk assessment tools and methodologies | Commission, MS and other stakeholders where relevant | ongoing |

Commissioning studies concerning interdependencies | Commission, MS and other stakeholders where relevant | ongoing |

Phase 2

Action | Actor | Timeframe |

Identification of gaps where Community initiatives would have added-value | Commission, MS and other stakeholders where relevant | ongoing |

Where relevant, setting up of CIP sector based expert groups at EU level | Commission, MS and other stakeholders where relevant | ongoing |

Identification of proposals for CIP actions that could be funded at EU level | Commission, MS | ongoing |

Initiation of EU funding for CIP actions | Commission | ongoing |

Phase 3

Action | Actor | Timeframe |

Initiation of cooperation with 3rd countries and international organisations; | Commission, MS | ongoing |

Work Stream 2. Protection of European critical infrastructure (ECI)

Work stream 2 will focus on reducing the vulnerability of ECI.

Phase 1

Action | Actor | Timeframe |

Elaboration of sector specific criteria to be used in identifying ECI | Commission, MS and other stakeholders where relevant | at the latest one year following the entry into force of the ECI Directive |

Phase 2

Action | Actor | Timeframe |

Identification and verification on a sector-by-sector basis of CI likely to qualify as ECI | Commission, MS | at the latest one year after the adoption of the relevant criteria and thereafter on an ongoing basis |

Designation of ECI | Commission, MS | ongoing |

Identification of vulnerabilities, threats and risks to particular ECI including the establishment of Operator Security Plans (OSPs) | Commission, MS, ECI owners/operators (generic report to Commission) | at the latest one year after designation as ECI |

Assessment of whether protection measures are

needed and whether EU level measures are required | Commission, MS and other stakeholders where relevant | at the latest 18 months after designation as ECI |

Assessment of the approach of each Member State to alert levels concerning infrastructure designated as ECI. Launching of a feasibility study on calibrating or harmonizing such alerts. | Commission, MS | ongoing |

Phase 3

Action | Actor | Timeframe |

Development and adoption of proposals for minimum protection measures concerning ECI | Commission, MS, ECI owners/operators | following the assessment of whether protection measures are needed and whether EU level measures are required |

Implementation of minimum protection measures | MS, ECI owners/operators | ongoing |

Work Stream 3. Support concerning NCI

Work Stream 3 is an intra-Member State work stream to assist the Member States in the protection of NCI.

Phase 1

Action | Actor | Timeframe |

Exchange of information on the criteria used to identify NCI | MS (Commission may assist where requested) | ongoing |

Phase 2

Action | Actor | Timeframe |

Identification and verification on a sector-by-sector basis of CI likely to qualify as NCI | MS and other stakeholders where relevant | ongoing |

Designation of particular CI as NCI | MS | ongoing |

Analysis of existing security gaps in relation to NCI on a sector-by-sector basis | MS and other stakeholders where relevant (Commission may assist where requested) | ongoing |

Phase 3

Action | Actor | Timeframe |

Establishment and development of National CIP Programmes | MS (Commission may assist where requested) | ongoing |

Development of specific protection measures for each NCI | MS, NCI (Commission may assist where requested) | ongoing |

Monitoring that owners/operators carry out the necessary implementation measures | MS | ongoing |

[1] The Commission intends to put forward a Communication on Protecting Europe's Critical Energy and Transport Infrastructure.

Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime

1. INTRODUCTION

1.1. What is cyber crime?

The security of the increasingly important information systems in our societies covers many aspects, of which the fight against cyber crime is a core element. Without an agreed definition of cyber crime, the terms "cyber crime", "computer crime", "computer-related crime" or "high-tech crime" are often used interchangeably. For the purpose of this Communication, 'cyber crime' is understood as "criminal acts committed using electronic communications networks and information systems or against such networks and systems".

In practice, the term cyber crime is applied to three categories of criminal activities. The first covers traditional forms of crime such as fraud or forgery, though in a cyber crime context relates specifically to crimes committed over electronic communication networks and information systems (hereafter: electronic networks). The second concerns the publication of illegal content over electronic media (i.a. child sexual abuse material or incitement to racial hatred). The third includes crimes unique to electronic networks , i.e. attacks against information systems, denial of service and hacking. These types of attacks can also be directed against the crucial critical infrastructures in Europe and affect existing rapid alert systems in many areas, with potentially disastrous consequences for the whole society. Common to each category of crime is that they may be committed on a mass-scale and with a great geographical distance between the criminal act and its effects. Consequently the technical aspects of applied investigative methods are often the same. These commonalities will form the focus of this Communication.

1.2. Latest developments in cyber crime

1.2.1. In general

The combination of constantly evolving criminal activities and a lack of reliable information makes it difficult to obtain an exact picture of the current situation. Nevertheless, some general trends can be discerned:

- The number of cyber crimes is growing and criminal activities are becoming increasingly sophisticated and internationalised[1]
- Clear indications point to a growing involvement of organised crime groups in cyber crime
- However, the number of European prosecutions on the basis of cross-border law enforcement cooperation do not increase

1.2.2. Traditional crime on electronic networks

Most crimes can be committed with the use of electronic networks, and different types of fraud and attempted fraud are particularly common and growing forms of crime on electronic networks. Instruments such as identity theft, phishing[2], spams and malicious codes may be used to commit large scale fraud. Illegal national and international Internet-based trade has also emerged as a growing problem. This includes trade in drugs, endangered species and arms.

1.2.3. Illegal content

A growing number of illegal content sites are accessible in Europe, covering child sexual abuse material, incitement to terrorist acts, illegal glorification of violence, terrorism, racism and xenophobia. Law enforcement action against such sites is extremely difficult, as site owners and administrators are often situated in countries other than the target country, and often outside the EU. The sites can be moved very quickly, also outside the territory of the EU, and the definition of illegality varies considerably from one state to another.

1.2.4. Crimes unique to electronic networks

Large scale attacks against information systems or organisations and individuals (often through so called botnets[3]) appear to have become increasingly prevalent. Also, incidents with systematic, well co-ordinated and large-scale direct attacks against the critical information infrastructure of a state have recently been observed. This has been compound-

ed by the merging technologies and accelerated interlinking of information systems, which rendered those systems more vulnerable. Attacks are often well organised and used for purposes of extortion. It can be assumed that the extent of reporting is minimised, in part due to the business disadvantages which may be the result if security problems were to become public.

1.3. Objectives

In the light of this changing environment, there is an urgent need to take action – at national as well as European level – against all forms of cyber crime, which are increasingly significant threats to critical infrastructures, society, business and citizens. Protection of individuals against cyber crime is often exacerbated by issues related to the determination of the competent jurisdiction, applicable law, cross-border enforcement or the recognition and use of electronic evidence. The essentially cross-border dimension of cyber crime highlights such difficulties. In addressing these threats, the Commission is launching a general policy initiative to improve European and international level coordination in the fight against cyber crime.

The objective is to strengthen the fight against cyber crime at national, European and international level. Further development of a specific EU policy, in particular, has long been recognised as a priority by the Member States and the Commission. The focus of the initiative will be on the law enforcement and criminal law dimensions of this fight and the policy will complement other EU actions to improve security in cyber space in general. The policy will eventually include: improved operational law enforcement cooperation; better political cooperation and coordination between Member States; political and legal cooperation with third countries; awareness raising; training; research; a reinforced dialogue with industry and possible legislative action.

The policy on the fight and prosecution of cyber crime will be defined and implemented in a manner fully respecting fundamental rights, in particular those of freedom of expression, respect for private and family life and the protection of personal data. Any legislative action taken in the context of this policy will be first scrutinised for compatibility with such rights, in particular the EU Charter of Fundamental Rights. It should also be noted that all such policy initiatives will be carried out in full consideration of Articles 12 to 15 of the so called e-commerce Directive[4], where this legal instrument applies.

The objective of this Communication can be divided into three main operational strands, which can be summarised as follows:

- To improve and facilitate coordination and cooperation between cyber crime units, other relevant authorities and other experts in the European Union
- To develop, in coordination with Member States, relevant EU and international organisations and other stakeholders, a coherent EU Policy framework on the fight against cyber crime
- To raise awareness of costs and dangers posed by cyber crime

2. EXISTING LEGAL INSTRUMENTS IN THE FIGHT AGAINST CYBER CRIME

2.1. Existing instruments and actions at EU level

The present Communication on cyber crime policy consolidates and develops the 2001 Communication on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime[5] (hereafter: the 2001 Communication). The 2001 Communication proposed appropriate substantive and procedural legislative provisions to deal with both domestic and trans-national criminal activities. From this, several important proposals followed. In particular, these include the proposal leading to the Framework Decision 2005/222/JHA on attacks against information systems[6]. In this context, it should also be noted that other, more general, legislation covering also aspects of the fight against cyber crime has been adopted, such as the Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment[7].

The Framework Decision 2004/68/JHA on sexual exploitation of children[8] is a good example of the particular focus put by the Commission on the protection of children , especially in relation to the fight against all forms of child sexual abuse material illegally published using information systems, a horizontal priority which will be kept in the future.

To tackle security challenges for the information society, the European Community has developed a three-pronged approach for network and information security: specific network and information security measures, the regulatory framework for electronic communications and the fight against cyber crime. Although these three aspects can, to a certain

extent, be developed separately, the numerous interdependencies call for tight coordination. In the related field of Network and Information security, a 2001 Commission Communication on Network and Information Security: A proposal for an EU policy approach[9], was adopted in parallel to the 2001 communication on cyber crime. The ePrivacy directive 2002/58/EC lays down an obligation for providers of publicly available electronic communication services to safeguard the security of their services. Provisions against spam and spyware are also laid down there. The Network and Information security policy has since been developed through a number of actions, most recently in Communications on a Strategy for a secure Information society[10] that sets out the revitalized strategy and provides the framework to carry forward and refine a coherent approach to Network and Information security, and on Fighting spam, spyware and malicious software[11], and in the 2004 creation of ENISA[12]. The main objective of ENISA is to develop expertise to stimulate cooperation between the public and private sectors, and provide assistance to the Commission and Member States. Research results in the area of technologies to secure information systems will also play an important role in the fight against cyber crime. Accordingly, Information and Communication Technologies as well as Security are all mentioned as objectives in the EU Seventh Research Framework Programme (FP 7), which will be operational during the period 2007-2013[13]. The review of the regulatory framework for electronic communications might result in amendments to to enhance the effectiveness of the security-related provisions of the ePrivacy Directive and the Universal Service Directive 2002/22/EC[14].

2.2. Existing international instruments

Due to the global nature of information networks, no policy on cyber crime can be effective if efforts are confined within the EU. Criminals can not only attack information systems or commit crimes from one Member State to another, but can easily do so from outside the EU's jurisdiction. Accordingly, the Commission has actively participated in international discussions and cooperation structures, i.a. the G 8 Lyon-Roma High-Tech Crime Group and Interpol-administered projects. The Commission is in particular closely following the work of the network for 24-hour contacts for International High-Tech Crime (the 24/7 network)[15], of which a considerable number of states worldwide, including most EU Member States, are members. The G8 network constitutes a mechanism to expedite contacts between participating states, with 24-hour points of contact for cases involving electronic evidence, and those requiring urgent assistance from foreign law enforcement authorities.

Arguably, the predominant European and international instrument in this field is the Council of Europe's 2001 Convention on cyber crime[16]. The Convention, which was adopted and entered into force in 2004, contains common definitions of different types of cyber crime and lays the foundation for a functioning judicial cooperation between contracting states. It has been signed by many states, including the United States of America and other non-European states, and by all Member States. A number of Member States have however not yet ratified the Convention or the additional protocol to the Convention dealing with acts of racist and xenophobic nature committed through computer systems. Considering the agreed importance of the Convention, the Commission will encourage Member States and relevant third countries to ratify the Convention and consider the possibility for the European Community to become a party to the Convention.

3. FURTHER DEVELOPMENT OF SPECIFIC INSTRUMENTS IN THE FIGHT AGAINST CYBER CRIME

3.1. Strengthening operational law enforcement cooperation and EU-level training efforts

The lack, or underutilisation, of immediate structures for cross-border operational cooperation remains a major weakness in the area of Justice, Freedom and Security. Traditional mutual assistance when confronted with urgent cyber crime cases has proven slow and ineffective, and new cooperation structures have not yet been sufficiently developed. While national judicial and law enforcement authorities in Europe cooperate closely via Europol, Eurojust and other structures, there remains an obvious need to strengthen and clarify responsibilities. Consultations undertaken by the Commission indicate that these crucial channels are not used in an optimal way. A more coordinated European approach must be both operational and strategic and also cover the exchange of information and best practices.

The Commission will in the near future lay particular emphasis on training needs. It is an established fact that the technological developments produce a need for continuous training on cyber crime issues for law enforcement and judicial authorities. A reinforced and better coordinated financial support from the EU to multinational training programs is therefore envisaged. The Commission will also, in

close cooperation with Member States and other competent organs such as Europol, Eurojust, the European Police College (CEPOL) and the European Judicial Training Network (EJNT), work to achieve an EU level coordination and interlinking of all relevant training programmes.

The Commission will organise a meeting of law enforcement experts from Member States, as well as from Europol, CEPOL and the EJTN, to discuss how to improve strategic and operational cooperation as well as cyber crime training in Europe in 2007. Among other things, the creation of both a permanent EU contact point for information exchange and an EU cyber crime training platform will be considered. The 2007 meeting will be the first in a series of meetings planned for the near future.

3.2. Strengthen the dialogue with industry

Both private and public sectors have an interest in jointly developing methods to identify and prevent harm resulting from the activities of crime. Shared private and public sector participation, based on mutual trust and a common objective of harm reduction, promises to be an effective way of enhancing security, also in the fight against cyber crime. The public-private aspects of the Commission's cyber crime policy will in time be part of a planned global EU policy on dialogue between the public and the private sector, covering the whole area of European security. This policy will in particular be taken forward by the European Security Research and Innovation Forum, which the Commission plans to create shortly and which will regroup relevant stakeholders from the public and the private sector.

The development of modern information technologies and electronic communication systems is largely controlled by private operators. Private companies carry out threat assessments, establish programmes for the fight against crime and develop technical solutions to prevent crime. Industry has displayed a very positive attitude to assisting public authorities in the fight against cyber crime, especially in efforts to counter child pornography[17] and other types of illegal content on the Internet.

Another issue concerns the apparent lack of exchange of information, expertise and best practices between the public and the private sector. Private sector operators are often, in order to protect business models and secrets, reluctant, or are under no clear legal obligation, to report or share relevant information on crime incidences with law enforcement authorities. However, such information may be needed if public authorities are to formulate an efficient and appropriate anti-crime policy. The possibilities to improve cross-sector information exchange will be considered also in the light of existing rules on protection of personal data.

The Commission already plays an important role in various public-private structures dealing with cyber crime, such as the Fraud Prevention Expert Group[18]. The Commission is convinced that an effective general policy for the fight against cyber crime must also include a strategy for cooperation between the public sector and private sector operators, including civil society organisations.

To achieve broader public-private cooperation in this field, the Commission will in 2007 organise a conference for law enforcement experts and private sector representatives, especially Internet Service Providers, to discuss how to improve public-private operational cooperation in Europe[19]. The conference will touch upon all subjects deemed to add value for both sectors, but especially:

- Improving operational cooperation in the fight against illegal activities and content on the Internet, specifically in the areas of terrorism, child sexual abuse material and other illegal activities particularly sensitive from a child protection perspective
- Initiating public-private agreements aiming at the EU-wide blocking of sites containing illegal content, especially child sexual abuse material
- Devising a European model for the sharing of necessary and relevant information across the private and public sectors, one consideration being to cultivate an atmosphere of mutual confidence and take the interests of all parties into account
- Establishing a network of law enforcement contact points in both private and public sectors

3.3. Legislation

General harmonisation of crime definitions and national penal laws in the field of cyber crime, is not yet appropriate, due to the variety of the types of offences covered by this notion. Since effective cooperation between law enforcement authorities often depends on having at least partly harmonised crime definitions, it remains a long-term objective to continue harmonising Member States' legislation[20]. With regard to certain key crime definitions,

an important step has already been taken with the Framework Decision on attacks against information systems. As described above, new threats have subsequently appeared and the Commission is closely following this evolution given the importance of continuously assessing the need for additional legislation. The monitoring of the evolving threats is closely coordinated with the European Programme for Critical Infrastructure Protection.

Targeted legislation against cyber crime should however also be considered now. A particular issue which may require legislation relates to a situation where cyber crime is committed in conjunction with identity theft . Generally, "identity theft" is understood as the use of personal identifying information, e.g. a credit card number, as an instrument to commit other crimes. In most Member States, a criminal would most likely be prosecuted for the fraud, or another potential crime, rather than for the identity theft; the former being considered a more serious crime. Identity theft as such is not criminalised across all Member States. It is often easier to prove the crime of identity theft than that of fraud, so that EU law enforcement cooperation would be better served were identity theft criminalised in all Member States. The Commission will in 2007 commence consultations to assess if legislation is appropriate.

3.4. Development of statistical data

It is generally agreed that the current state of information concerning the prevalence of crime is largely inadequate, and in particular that much improvement is needed to compare data between Member States. An ambitious five-year plan to tackle this problem was set out in the Communication from the Commission on Developing a comprehensive and coherent EU strategy to measure crime and criminal justice: An EU Action Plan 2006 – 2010 [21]. The Expert Group set up under this Action Plan would provide a suitable forum for developing relevant indicators for measuring the extent of cyber crime.

4. THE WAY FORWARD

The Commission will now take the general policy for the fight against cyber crime forward. Due to the limited powers of the Commission in the field of criminal law, this policy can only be a complement to the actions undertaken by Member States and other bodies. The most important actions – each of which will imply the use of one, several or all of the instruments presented in Chapter 3 – will also be supported through the Financial Programme "Prevention of and Fight against Crime":

4.1. The fight against cyber crime in general

- Establish a strengthened operational cooperation between Member States' law enforcement and judicial authorities, an action which will begin with the organisation of a dedicated expert meeting in 2007 and which may include the setting up of a central EU cyber crime contact point
- Increase financial support to initiatives for improved training of law enforcement and judicial authorities vis-à-vis the handling of cyber crime cases and take action to coordinate all multinational training efforts in this field by the setting up of an EU training platform
- Promote a stronger commitment from Member States and all public authorities to take effective measures against cyber crime and to allocate sufficient resources to combat such crimes
- Support research beneficial to the fight against cyber crime
- Organise at least one major conference (in 2007) with law enforcement authorities and private operators, especially to initiate cooperation in the fight against illegal Internet activities in and against electronic networks and to promote a more effective non-personal information exchange, and to follow-up on the conclusions from this 2007 conference with concrete public-private cooperation projects
- Take the initiative for and participate in public-private actions aimed at raising awareness, especially among consumers, of the cost of and dangers posed by cyber crime, while avoiding the undermining of the trust and confidence of consumers and users by focusing only on negative aspects of security
- Actively participate in and promote global international cooperation in the fight against cyber crime
- Initiate, contribute to and support international projects which are in line with the Commission policy in this field, e.g. projects run by the G 8 and consistent with the Country and Regional Strategy Papers (regarding cooperation with third countries)
- Take concrete action to encourage all Member States and relevant third countries to

ratify the Council of Europe's Cyber Crime Convention and its additional protocol and consider the possibility for the Community to become a party to the Convention

- Examine, together with the Member States, the phenomenon of co-ordinated and large scale attacks against the information infrastructure of member states in view of preventing and combating these, including co-ordinating responses, and sharing information and best practices

4.2. Fight against traditional crime in electronic networks

- Initiate an in-depth analysis with a view to preparing a proposal for specific EU legislation against identity theft
- Promote the development of technical methods and procedures to fight fraud and illegal trade on the Internet, also through public-private cooperation projects
- Continue and develop work in specific targeted areas, such as in the Fraud Prevention Expert Group on the fight against fraud with non-cash means of payment in electronic networks

4.3. Illegal content

- Continue to develop actions against specific illegal content, especially regarding child sexual abuse material and incitement to terrorism and notably through the follow-up of the implementation of the Framework Decision on sexual exploitation of children
- Invite the Member States to allocate sufficient financial resources to strengthen the work of law enforcement agencies with special attention to identifying the victims of sexual abuse material which is distributed online
- Initiate and support actions against illegal content that may incite minors to violent and other serious illegal behaviour, i.a. certain types of extremely violent on-line video games
- Initiate and promote dialogue between Member States and with third countries on technical methods to fight illegal content as well as on procedures to shut down illegal websites, also with a view to the possible development of formal agreements with neighbouring and other countries on this issue
- Develop EU-level voluntary agreements and conventions between public authorities and private operators, especially Internet service providers, regarding procedures to block and close down illegal Internet sites

4.4. Follow-up

In this Communication, a number of actions aimed at improving cooperation structures in the EU have been outlined as next steps. The Commission will take these actions forward, assess progress on the implementation of the activities, and report to the Council and Parliament.

[1] The majority of this Communication's statements on current trends have been taken from the Study to assess the impact of a communication on cyber crime, ordered by the Commission in 2006 (Contract No JLS/2006/A1/003).

[2] Phishing describes attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person in an electronic communication.

[3] Botnet refers to a collection of compromised machines running programs under a common command.

[4] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178, 17.7.2000, p. 1).

[5] COM(2000) 890, 26.1.2001.

[6] OJ L 69, 16.3.2005, p. 67.

[7] OJ L 149, 2.6.2001, p. 1.

[8] OJ L 13, 20.1.2004, p. 44.

[9] COM(2001) 298.

[10] COM(2006) 251.

[11] COM(2006) 688.

[12] Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency (OJ L 77, 13.3.2004, p. 1).

[13] The European Union has already under the 6th Framework Programme for Research and and Technological development supported a number of relevant, and successful, research projects.

[14] COM(2006) 334, SEC(2006)816, SEC(2006) 817.

[15] See Article 35 in the Council of Europe Convention on cyber crime.

[16] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[17] One recent example of cooperation in this field is the cooperation between law enforcement and credit-card companies, through which the latter have assisted the police in tracking down purchasers of online child pornography.

[18] See http://ec.europa.eu/internal_market/payments/fraud/index_en.htm

[19] The Conference could be regarded as the continuation of the EU Forum presented in Section 6.4 in the computer-crime communication.

[20] This longer-term objective has already been mentioned on page 3 of the 2001 Communication.

[21] COM(2006) 437, 7.8.2006.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"

1. INTRODUCTION

Information and Communication Technologies (ICTs) are increasingly intertwined in our daily activities. Some of these ICT systems, services, networks and infrastructures (in short, ICT infrastructures) form a vital part of European economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures. They are typically regarded as critical information infrastructures (CIIs)[1] as their disruption or destruction would have a serious impact on vital societal functions. Recent examples include the large-scale cyber-attacks targeting Estonia in 2007 and the breaks of transcontinental cables in 2008.

The World Economic Forum estimated in 2008 that there is a 10 to 20% probability of a major CII breakdown in the next 10 years, with a potential global economic cost of approximately 250 billion US$.[2]

This Communication focuses on prevention, preparedness and awareness and defines a plan of immediate actions to strengthen the security and resilience of CIIs. This focus is consistent with the debate launched at the request of the Council and the European Parliament to addresses the challenges and priorities for network and information security (NIS) policy and the most appropriate instruments needed at EU level to tackle them. The proposed actions are also complementary to those to prevent, fight and prosecute criminal and terrorist activities targeting CIIs and synergetic with current and prospective EU research efforts in the field of network

and information security, as well as with international initiatives in this area.

2. THE POLICY CONTEXT

This Communication develops the European policy to strengthen the security of and the trust in the information society. Already in 2005, the Commission[3] highlighted the urgent need to coordinate efforts to build trust and confidence of stakeholders in electronic communications and services. To this end a strategy for a secure information society[4] was adopted in 2006. Its main elements, including the security and resilience of ICT infrastructures, were endorsed in Council Resolution 2007/068/01. However, ownership and implementation by stakeholders appear insufficient. This strategy also strengthens the role, on tactical and operational levels, of the European Network and Information Security Agency (ENISA), established in 2004 to contribute to the goals of ensuring a high and effective level of NIS within the Community and developing a culture of NIS for the benefit of EU citizens, consumers, enterprises and administrations.

In 2008 ENISA's mandate was extended 'à l'identique' until March 2012.[5] At the same time, the Council and the European Parliament called for "further discussion on the future of ENISA and on the general direction of the European efforts towards an increased network and information security." To support this debate, the Commission launched last November an on-line public consultation,[6] the analysis of which will be made available shortly.

The activities planned in this Communication are conducted under and in parallel to the European Programme for Critical Infrastructure Protection (EPCIP)[7]. A key element of EPCIP is the Directive[8] on the identification and designation of European Critical Infrastructures,[9] which identifies the ICT sector as a future priority sector. Another important element of EPCIP is the Critical Infrastructure Warning Information Network (CIWIN).[10]

On the regulatory side, the Commission proposal to reform the Regulatory Framework for electronic communications networks and services[11] contains new provisions on security and integrity, in particular to strengthen operators' obligations to ensure that appropriate measures are taken to meet identified risks, guarantee the continuity of supply of services and notify security breaches.[12] This approach is conducive to the general objective of enhancing the security and resilience of CIIs. The European Parliament and the Council broadly support these provisions.

The actions proposed in this Communication complement existing and prospective measures in the area of police and judicial cooperation to prevent, fight and prosecute criminal and terrorist activities targeting ICT infrastructures, as envisaged inter alia by the Council Framework Decision on attacks against information systems[13] and its planned update.[14]

This initiative takes into account NATO activities on common policy on cyber defence, i.e. the Cyber Defence Management Authority and the Cooperative Cyber Defence Centre of Excellence.

Lastly, due account is given to international policy developments, in particular to the G8 principles on CIIP[15]; the UN General Assembly Resolution 58/199 Creation of a global culture of cybersecurity and the protection of critical information infrastructures and the recent OECD Recommendation on the Protection of Critical Information Infrastructures.

3. WHAT IS AT STAKE

3.1. Critical information infrastructures are vital for the economy and societal growth of the EU

The economic and societal role of the ICT sector and ICT infrastructures is highlighted in recent reports on innovation and economic growth. This includes the Communication on i2010 mid-term review[16], the Aho Group report[17] and the European Union yearly economic reports.[18] The OECD underlines the importance of ICTs and the Internet " to boost economic performance and social well-being, and to strengthen societies' capacity to improve the quality of life for citizens worldwide "[19]. It further recommends policies that strengthen confidence in the Internet infrastructure.

The ICT sector is vital for all segments of society. Businesses rely on the ICT sector both in terms of direct sales and for the efficiency of internal processes. ICTs are a critical component of innovation and are responsible for nearly 40% of productivity growth.[20] ICTs are also pervasive for the work of governments and public administrations: the uptake of eGovernment services at all levels, as well as new applications such as innovative solutions related to health, energy and political participation, make the public sector heavily dependent on ICTs. Last, not least, citizens increasingly rely on and use ICTs in their daily activities: strengthening CII security would increase citizens' trust in ICTs, not least thanks to a better pro-

tection of personal data and privacy.

3.2. The risks to critical information infrastructures

The risks due to man-made attacks, natural disasters or technical failures are often not fully understood and/or sufficiently analysed. Consequently, the level of awareness across stakeholders is insufficient to devise effective safeguards and countermeasures.

Cyber-attacks have risen to an unprecedented level of sophistication. Simple experiments are now turning into sophisticated activities performed for profit or political reasons. The recent large scale cyber-attacks on Estonia, Lithuania and Georgia are the most widely covered examples of a general trend. The huge number of viruses, worms and other forms of malware, the expansion of botnets and the continuous rise of spam confirm the severity of the problem. [21]

The high dependence on CIIs, their cross-border interconnectedness and interdependencies with other infrastructures, as well as the vulnerabilities and threats they face raise the need to address their security and resilience in a systemic perspective as the frontline of defence against failures and attacks.

3.3. Security and resilience of critical information infrastructures to boost confidence in the information society

In order to ensure that ICT infrastructures are used to their maximum extent, thus fully realising the economic and social opportunities of the information society, all stakeholders must have a high level of confidence and trust in them. This depends on various elements, the most important of which is ensuring their high level of security and resilience. Diversity, openness, interoperability, usability, transparency, accountability, auditability of the different components and competition are key drivers for security development and stimulate the deployment of security-enhancing products, processes and services. As the Commission already highlighted[22], this is a shared responsibility: no single stakeholder has the means to ensure the security and resilience of all ICT infrastructures and to carry all the related responsibilities.

Taking up such responsibilities calls for a risk management approach and culture, able to respond to known threats and anticipate unknown future ones, without over-reacting and stifling the emergence of innovative services and applications.

3.4. The challenges for Europe

In addition and complementarily to all the activities related to the implementation of the Directive on the identification and designation of the European Critical Infrastructures, in particular the identification of ICT sector-specific criteria, a number of broader challenges need to be addressed in order to strengthen the security and resilience of CIIs.

3.4.1. Uneven and uncoordinated national approaches

Although there are commonalities among the challenges and the issues faced, measures and regimes to ensure the security and resilience of CIIs, as well as the level of expertise and preparedness, differ across Member States.

A purely national approach runs the risk of producing a fragmentation and inefficiency across Europe. Differences in national approaches and the lack of systematic cross-border co-operation substantially reduce the effectiveness of domestic countermeasures, inter alia because, due to the interconnectedness of CIIs, a low level of security and resilience of CIIs in a country has the potential to increase vulnerabilities and risks in other ones.

To overcome this situation a European effort is needed to bring added value to national policies and programmes by fostering the development of awareness and common understanding of the challenges; stimulating the adoption of shared policy objectives and priorities; reinforcing cooperation between Member States and integrating national policies in a more European and global dimension.

3.4.2. Need for a new European governance model for CIIs

Enhancing the security and the resilience of CIIs poses peculiar governance challenges. While Member States remain ultimately responsible for defining CII-related policies, their implementation depends on the involvement of the private sector, which owns or controls a large number of CIIs. On the other hand, markets do not always provide sufficient incentives for the private sector to invest in the protection of CIIs at the level that governments would normally demand.

To address this governance problem public-private partnerships (PPPs) have emerged at the national level as the reference model. However, despite the consensus that PPPs would also be desirable on a

European level, European PPPs have not materialised so far. A Europe-wide multi-stakeholder governance framework, which may include an enhanced role of ENISA, could foster the involvement of the private sector in the definition of strategic public policy objectives as well as operational priorities and measures. This framework would bridge the gap between national policy-making and operational reality on the ground.

3.4.3. Limited European early warning and incident response capability

Governance mechanisms will be truly effective only if all participants have reliable information to act upon. This is particularly relevant for governments that have the ultimate responsibility to ensure the security and well-being of citizens.

However, processes and practices for monitoring and reporting network security incidents differ significantly across Member States. Some do not have a reference organisation as a monitoring point. More importantly, cooperation and information sharing between Member States of reliable and actionable data on security incidents appears underdeveloped, being either informal or limited to bilateral or limitedly multilateral exchanges. In addition, simulating incidents and running exercises to test response capabilities are strategic in enhancing the security and resilience of CIIs, in particular by focusing on flexible strategies and processes for dealing with the unpredictability of potential crises. In the EU, cybersecurity exercises are still in an embryonic state. Exercises running across national boundaries are very limited. As recent events[23] showed, mutual aid is an essential element of a proper response to large-scale threats and attacks to CIIs.

A strong European early warning and incident response capability has to rely on well-functioning National/Governmental Computer Emergency Response Teams (CERTs), i.e. having a common baseline in terms of capabilities. These bodies need to act as national catalysers of stakeholders' interests and capacity for public policy activities (including those related to information and alert sharing systems reaching out to citizens and SMEs) and to engage in effective cross-border cooperation and information exchange, possibly leveraging existing organisations such as the European Governmental CERTs Group (EGC).[24]

3.4.4. International cooperation

The rise of the Internet as a key CII requires particular attention to its resilience and stability. The Internet, thanks to its distributed, redundant design has proven to be a very robust infrastructure. However, its phenomenal growth produced a rising physical and logical complexity and the emergence of new services and uses: it is fair to question the capability of the Internet to withstand the rising number of disruptions and cyber-attacks.

The divergence of views on the criticality of the elements making up the Internet partly explains the diversity of governmental positions expressed in international fora and the often contradicting perceptions of the importance of this matter. This could hinder a proper prevention of, preparedness for and ability to recover from threats affecting the Internet. For example, the consequences of the transition from IPv4 to IPv6 should also be assessed in terms of CII security.

The Internet is a global and highly distributed network of networks, with control centres not necessarily following national boundaries. This calls for a specific, targeted approach in order to ensure its resilience and stability, based on two converging measures. First, achieving a common consensus on the European priorities for the resilience and stability of the Internet, in terms of public policy and of operational deployment. Secondly, engaging the global community to develop a set of principles, reflecting European core values, for Internet resilience and stability, in the framework of our strategic dialogue and cooperation with third countries and international organisations. These activities would build upon the recognition by the World Summit on Information Society[25] of the key importance of the stability of the Internet.

4. THE WAY FORWARD: TOWARDS MORE EU COORDINATION AND COOPERATION

Because of the Community and international dimension of the problem an integrated EU approach to enhance the security and resilience of CIIs would complement and add value to national programmes as well as to the existing bilateral and multilateral cooperation schemes between Member States.

Public policy discussions in the aftermath of the events in Estonia suggest that the effects of similar attacks can be limited by preventive measures and by coordinated action during the actual crisis. A more structured exchange of information and good practices across the EU could considerably facilitate fighting cross-border threats.

It is necessary to strengthen the existing instruments for cooperation, including ENISA, and, if necessary, create new tools. A multi-stakeholder, multi-level approach is essential, taking place at the European level while fully respecting and complementing national responsibilities.

A thorough understanding of the environment and constraints is necessary. For example, the distributed nature of the Internet, where edge nodes can be used as vectors of attack, e.g. botnets, is a concern. However, this distributed nature is a key component of stability and resilience and can help a faster recovery than would normally be the case with over-formalised, top-down procedures. This calls for a cautious, case-by-case analysis of public policies and operational procedures to put in place.

The time horizon is also important. There is a clear need to act now and put rapidly in place the necessary elements to build a framework that will enable us to respond to current challenges and that will feed into the future strategy for network and information security.

Five pillars are proposed to tackle these challenges:

1. Preparedness and prevention: to ensure preparedness at all levels;
2. Detection and response: to provide adequate early warning mechanisms;
3. Mitigation and recovery: to reinforce EU defence mechanisms for CII;
4. International cooperation: to promote EU priorities internationally;
5. Criteria for the ICT sector: to support the implementation of the Directive on the Identification and Designation of European Critical Infrastructures[26].

5. THE ACTION PLAN

5.1. Preparedness and prevention

Baseline of capabilities and services for pan-European cooperation. The Commission invites Member States and concerned stakeholders to

- define, with the support of ENISA, a minimum level of capabilities and services for National/Governmental CERTs and incident response operations in support to pan-European cooperation.
- make sure National/Governmental CERTs act as the key component of national capability for preparedness, information sharing, coordination and response.

Target: end of 2010 for agreeing on minimum standards; end of 2011 for establishing well functioning National/Governmental CERTs in all Member States.

European Public Private Partnership for Resilience (EP3R). The Commission will

- foster the cooperation between the public and the private sector on security and resilience objectives, baseline requirements, good policy practices and measures. The primary focus of the EP3R would be on the European dimension from strategic (e.g. good policy practices) and tactical/operational (e.g. industrial deployment) perspectives. EP3R should build upon and complement existing national initiatives and the operational activities of ENISA.

Target: end of 2009 for a roadmap and plan for EP3R; mid of 2010 for establishing EP3R; end of 2010 for EP3R to produce its first results.

European Forum for information sharing between Member States. The Commission will

- establish a European Forum for Member States to share information and good policy practices on security and resilience of CIIs. This would benefit from the results of the activities of other organisations, in particular ENISA.

Target: end of 2009 for launching the Forum; end of 2010 for delivering the first results.

5.2. Detection and response

European Information Sharing and Alert System (EISAS). The Commission supports

the development and deployment of EISAS, reaching out to citizens and SMEs and being based on national and private sector information and alert sharing systems. The Commission financially supports two complementary prototyping projects. [27] ENISA is called upon to take stock of the results of these projects and other national initiatives and produce a roadmap to further the development and deployment of EISAS.

Target: end of 2010 for completing the prototyping projects; end of 2010 for the roadmap towards a Eu-

ropean- system.

5.3. Mitigation and recovery

National contingency planning and exercises. The Commission invites Member States to

- develop national contingency plans and organise regular exercises for large scale networks security incident response and disaster recovery, as a step towards closer pan-European coordination. National/Governmental CERTs/CSIRTs may be tasked to lead national contingency planning exercises and testing, involving private and public sector stakeholders. The involvement of ENISA is called upon to support the exchange of good practices between Member States.

Target: end of 2010 for running at least one national exercise in every Member State.

Pan-European exercises on large-scale network security incidents. The Commission will

- financially support the development of pan-European exercises on Internet security incidents,[28] which may also constitute the operational platform for pan-European participation in international network security incidents exercises, like the US Cyber Storm.

Target: end of 2010 for the design and run of the first pan-European exercise; end of 2010 for pan-European participation in international exercises.

Reinforced cooperation between National/Governmental CERTs. The Commission invites Member States to

- strengthen the cooperation between National/Governmental CERTs, also by leveraging and expanding existing cooperation mechanisms like the EGC.[29] The active role of ENISA is called upon to stimulate and support pan-European cooperation between National/Governmental CERTs that should lead to enhanced preparedness; reinforced European capacity to react and respond to incidents; pan-European (and/or regional) exercises.

Target: end of 2010 for doubling the number of national bodies participating in ECG; end of 2010 for ENISA to develop reference materials to support pan-European cooperation.

5.4. International cooperation

Internet resilience and stability. Three complementary activities are envisaged

- *European priorities on long term Internet resilience and stability.* The Commission will drive a Europe-wide debate, involving all relevant public and private stakeholders, to define EU priorities for the long term resilience and stability of the Internet.

Target: end of 2010 for EU priorities on critical Internet components and issues.

- *Principles and guidelines for Internet resilience and stability (European level).* The Commission will work with Member States to define guidelines for the resilience and stability of the Internet, focusing inter alia on regional remedial actions, mutual assistance agreements, coordinated recovery and continuity strategies, geographical distribution of critical Internet resources, technological safeguards in the architecture and protocols of the Internet, replication and diversity of services and data. The Commission is already funding a task force for DNS resiliency that, together with other relevant projects, will help build the consensus.[30]

Target: end of 2009 for a European roadmap towards principles and guidelines for Internet resilience and stability; end of 2010 for agreeing on the first draft of such principles and guidelines.

- *Principles and guidelines for Internet resilience and stability (global level).* The Commission will work with Member States on a roadmap to promote principles and guidelines at the global level. Strategic cooperation with third countries will be developed, notably in Information Society dialogues, as a vehicle to build global consensus.[31]

Target: beginning of 2010 for a roadmap for international cooperation on principles and guidelines for security and resilience; end of 2010 for the first draft of internationally recognised principles and guidelines to be discussed with third countries and in relevant fora, including the Internet Governance Forum.

Global exercises on recovery and mitigation of large scale Internet incidents. The Commission invites European stakeholders to

- reflect on a practical way to extend at the

global level the exercises being conducted under the mitigation and recovery pillar, building upon regional contingency plans and capabilities.

Target: end of 2010 for the Commission to propose a framework and a roadmap to support the European involvement and participation in global exercises on recovery and mitigation of large-scale Internet incidents.

5.5. Criteria for European Critical Infrastructures in the ICT sector

ICT sector specific criteria. By building on the initial activity carried out in 2008, the Commission will

- continue to develop, in cooperation with Member States and all relevant stakeholders, the criteria for identifying European critical infrastructures for the ICT sector. To this end, relevant information will be drawn from a specific study being launched.[32]

Target: first half of 2010 for the Commission to define the criteria for the European critical infrastructures for the ICT sector.

6. CONCLUSIONS

Security and resilience of CIIs are the frontline of defence against failures and attacks. Their enhancement across the EU is essential to reap the full benefits of the information society. To achieve this ambitious objective an action plan is proposed to reinforce the tactical and operational cooperation at the European level. The success of these actions depends on their effectiveness to build upon and benefit public and private sector's activities, on the commitment and full participation of Member States, European Institutions and stakeholders.

To this end, a Ministerial Conference will take place on 27-28 April 2009 to discuss the proposed initiatives with Member States and to mark their commitment to the debate on a modernised and reinforced NIS policy in Europe.

Lastly, enhancing the security and resilience of CIIs is a long term objective, whose strategy and measures need regular assessments. Therefore, since this goal is consistent with the general debate on the future of network and information security policy in the EU after 2012, the Commission will initiate a stock-taking exercise toward the end of 2010, in order to evaluate the first phase of actions and to identify and propose further measures, as appropriate.

[1] A definition of CIIs was proposed in COM(2005) 576 final

[2] Global Risks 2008

[3] COM(2005) 229

[4] COM(2006) 251

[5] Regulation (EC) No 1007/2008

[6] http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464

[7] COM(2006) 786 final

[8] 2008/114/EC

[9] http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/gena/104617.pdf

[10] COM(2008) 676 final

[11] COM(2007) 697, COM(2007) 698, COM(2007) 699

[12] Art. 13 Framework Directive

[13] 2005/222/JHA

[14] COM(2008) 712

[15] http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf

[16] COM(2008) 199 final

[17] http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm

[18] EU Economy 2007 Review http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf

[19] http://www.oecd.org/dataoecd/1/29/40821707.pdf

[20] http://epp.eurostat.ec.europa.eu/ - Science and Technology/Information Society

[21] COM(2006) 688 final

[22] COM(2006) 251 final

[23] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/

[24] http://www.egc-group.org/

[25] Tunis Agenda for the Information Society, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

[26] Council Directive 2008/114/EC

[27] Under the EC Programme " Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks " http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm

[28] Supra 27

[29] Supra 24

[30] Supra 27

[31] COM(2008)588 final

[32] Supra 27

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Final evaluation of the implementation of the multiannual Community Programme on promoting safer use of the Internet and new online technologies

1. INTRODUCTION

This Communication concerns the final evaluation of the multiannual Safer Internet plus programme (2005-2008) referred to in this communication as "the programme".

The objective of the programme, as specified in the European Parliament and Council Decision[1], was promoting safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end-user.

The programme ran over a four-year period from 1 January 2005 to 31 December 2008 with a reference budget of 45 million euro.

The programme was implemented through four main action lines:

- fighting against illegal content;
- tackling unwanted and harmful content;
- promoting a safer environment;
- awareness-raising.

By comparison with the preceding Safer Internet Action Plan, the coverage was extended to include online technologies, including mobile and broadband content, online games, peer-to-peer file transfer, and all forms of real-time communications such as chat rooms and instant messages primarily with the aim of improving the protection of children and minors. A broader range of areas of illegal and harmful content and conduct of concern were covered, including racism and violence.

The main mechanism for implementing the programme has been the co-financing of projects selected on the basis of public calls for proposals. This has resulted in a wide range of projects being funded under the various action lines, complemented by non-funded activities as appropriate.

The programme co-funds the INSAFE network of awareness nodes for carrying out awareness actions designed to reach children, families and schools, and helplines where children can raise concerns related to their use of online technologies, and the INHOPE network of hotlines allowing internet users to report illegal content[2].

The programme further supports thematic networks bringing together different stakeholders such as researchers, non-governmental organisations (NGOs) and law enforcement agencies in order to facilitate dialogue and exchange of best practice, targeted projects aiming at enhancing the analysis of illegal material by law enforcement agencies and projects for knowledge enhancement on various aspects of children's, parents and offenders' use of the Internet. The EU Kids Online project provides new knowledge about children's and parent's experiences of risk and safety, and a successor project will address the lack of comparative data which this has identified. A second project will enhance the knowledge of online-related sexual abuse of children by conducting qualitative research into adult offending.[3]

Two Eurobarometer surveys, with the purpose of exploring the attitude of EU citizens towards illegal and harmful content and their knowledge of how to protect themselves, were conducted under the auspices of the programme and a further survey will be carried out during autumn 2008.

In addition, the Commission has carried out a study into the effectiveness of filtering software. Among other results of the Programme, Safer Internet Day is celebrated world-wide in February and 56 countries took part in 2008. The Commission has instituted a dialogue with industry and civil society to foster self-regulation. The mobile phone industry adopted a European Framework for Safer Mobile use by younger teenagers and children in 2007. The annual Safer Internet Forum is a recognised meeting-point for all stakeholders, with discussion of topical issues.

According to Article 5 of the Programme Decision, the Commission shall submit to the European Parliament and the Council, at the end of the programme, a final evaluation report on the results obtained in implementing the programme.

The evaluation was conducted by a panel of three independent experts[4] during the period May to July 2008, in close collaboration with the Commission services concerned[5].

2. EVALUATION OBJECTIVES

The evaluation assessed the following specific issues: relevance of the programme's objectives, priorities and means of implementation, the effectiveness of the programme, its achievements, its impact, its sustainability and its complementarity with other initiatives within and external to the European Union, as well as with national initiatives.

3. EVALUATION FINDINGS

The evaluators found that the programme has been successful in achieving the stated objectives as set out in the original Programme Decision and in subsequent annual work programmes. It has contributed to achieving a safer Internet through a range of interventions and produced a significant impact and influence. Feedback from stakeholders shows clear appreciation of the programme, particularly the knowledge sharing opportunities which it provides, and in emphasizing the importance of the work continuing.

More specifically it was concluded that:

The Commission has been able to adapt the priorities of the programme to respond to changing challenges and needs and that the programme has managed successfully to ensure that the themes and actions are relevant to the dynamic social and technological environment within which it operates.

The geographical scope of the programme is another area where the programme has responded in a timely and effective way. The rapid geographic growth of the EU has been mirrored quickly to include new member states in its activities.

The programme has further a high degree of relevance in its recent focus on consulting children and young people and ensuring that both their rights and their opinions are a priority within all aspects of the programme.

The management of the programme has been efficient and effective. There are hotlines and awareness nodes in almost all members states, a number of thematic networks have been established, and work is continuing on developing technical solutions in areas such as image recognition. However, the detailed level of effectiveness within the broad programme objectives has been more difficult to quantify, and it is important to collect and analyse more measurable data in follow-up initiatives in order to ensure the effectiveness and impact of funded activities.

The programme demonstrates considerable achievements . Not only has it continued to keep the issue of safer Internet high on the agenda of policy makers across Europe and beyond, but it has also become a driver for action outside the European context. The programme's experiences and best practices are seen as very helpful and stimulating by other countries which are confronted by similar challenges. The very broad international membership of INHOPE is also a testament to the standing of the programme in the wider internet community.

The networking opportunity provided by the programme is highly valued by many stakeholders, who emphasize the fact that the programme enables sectors to work together who would otherwise not have joined forces, for example major telecoms providers and NGOs.

The expansion of the two networks to cover virtually the whole European area as well as countries further afield is an undoubted achievement. The INSAFE network has grown from a coverage of 21 countries in 2006 to 34 countries in 2008. The INHOPE network has had a similar growth, with 13 members joining during the period of the programme, bringing the total membership to 33.

Another achievement is the extent to which the programme has encouraged collection and analysis of a huge body of research of safer Internet issues by the EU Kids Online network.

Successful work has been undertaken in the area of fostering dialogue within and between different sectors, and in encouraging the mobile phone industry in its efforts to adopt effective self-regulatory mechanisms on protecting minors.

As regards the awareness activities, the Safer Internet Day has been an undoubted success – the event has grown in terms of numbers and geographical scope year on year, with an increasingly interna-

tional focus and impressive level press and media coverage.

In terms of the impact of the programme the consistent approach and messages across Europe are an important factor for the high level of success of the programme.

However, the visibility of the programme would be enhanced by greater online and offline presence and promotion. A greater consistency in branding would assist in establishing the identity and credibility of the programme within different sectors, countries and regions.

The sustainability of the programme itself is robust . It is, however, important to monitor the function of the networks to ensure that the model is still the most appropriate one. In particular, the requirement for hotlines, awareness nodes and helplines to form combined nodes at the national level in order to increase effectiveness and efficiency also raises the question of whether the two networks should be required to combine in a single organisation to co-ordinate all activities across Europe.

The programme offers complementarity with a range of initiatives within and external to the EU as well as with national initiatives within most member states , particularly with regard to fighting illegal content, promoting media literacy and affirming children's rights.

There is a clear emphasis among stakeholders on the importance of the programme as a catalyst for international and national involvement. Where there was no previous national engagement, it helped to put the issues on the agenda and bring stakeholders to the table. In countries where organisations had already started working on these issues, the programme helped to co-ordinate the approach and gave credibility to organisations that might otherwise have found it difficult to get the attention of national authorities and industry.

4. EVALUATION RECOMMENDATIONS

The evaluation report makes a number of recommendations to be taken into account for future work:

1. The rights and privacy of children, young people and other legitimate Internet users should be protected and promoted within all activities of the Programme. The involvement of young people themselves in discussion, design and delivery of solutions could be further intensified.
2. Continued efforts could be made to achieve active support and involvement for the Programme and individual projects on a national level from all relevant sectors. This should be reflected in the creation of multi-stakeholder networks at the European level in order to bring together different constituencies.
3. Co-operation and collaboration with third countries, both within and outside Europe, on a policy and operational level should be given a high priority, particularly with regard to identifying, tracing and eradicating illegal child abuse images.
4. Enhanced dialogue and cooperation should be established among the various EU initiatives with an intersection of interests or the potential for collaboration with the Safer Internet plus programme in order to identify new areas of synergy and innovation and to improve the effectiveness of the individual programmes.
5. Future solutions should continue to take into account national, cultural, linguistic and socio-demographic factors, particularly for new, candidate and accession countries, to ensure that interventions are relevant and valid.
6. The technical knowledge base of the Programme should be further strengthened in order to retain a high level of current knowledge and credibility.
7. The Programme would probably benefit from a more consistent 'brand' with quality control measures in place for internal and partner websites and other resources. More proactive use should be made of the press and media across Europe.
8. Further knowledge enhancement activity could be conducted in two key areas: problematic, risky and criminal online behaviours on the part of children and young people themselves; the underlying reasons for the trends identified by INHOPE in respect of illegal content.
9. The roles of the two networks (INHOPE and INSAFE) should be re-visited to ensure they offer the most appropriate mechanism for co-ordinating the work of national nodes. Consideration should be given to the question of whether the two networks should be merged to reflect the emphasis on combined hotline, awareness and helpline activity and to deal adequately with the planned extension of the scope of the programme to include cyber-bullying and

grooming.

10. A high priority should be given to raising the visibility of hotlines, which still suffer from low levels of public awareness. The visibility of helplines also needs attention in order to provide European citizens with appropriate contact points, and to complement the work of the hotlines by dealing with issues of a broader nature.

11. The Programme could engage more actively with industry. Priority should be given to establishing a common code of practice among Internet Service Providers throughout Europe, along the lines of the Framework Agreement signed by mobile network operators.

5. COMMISSION COMMENTS AND CONCLUSION

The Commission takes full note of the findings of the final evaluation of the programme and will take the recommendations into account when implementing the follow-up programme. Progress already made in areas mentioned by the recommendations will be reinforced.

In the light of the Commission's responses to the evaluators' report, it invites the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions to:

12. Take note that the programme has been successfully implemented;

13. Assist the Commission in its work of increasing the visibility of the Safer Internet programme and stimulate a continued dialogue on safer Internet issues.

[1] Decision No. 854/2005/EC of 11 May 2005 of the European Parliament and of the Council published in OJ L149 of 11.6.2005, p. 1

[2] By the end of 2008, taking account of projects under negotiation, there will be 27 awareness nodes in 25 Member States and Iceland and Norway, 21 helplines and 24 hotlines.

[3] A full list of projects co-funded by the programme can be found at http://ec.euroapa.eu/saferinternet

[4] The experts were appointed on the basis of a restricted call for tenders launched in spring 2008.

[5] DG INFSO Units C3 and E6

GROUP OF EIGHT

Meeting of Justice and Interior Ministers of The Eight (December 9-10, 1997). COMMUNIQUÉ, WASHINGTON, D.C., DECEMBER 10

At the Summit of The Eight in Denver, our Heads of State and Government directed us to intensify our efforts to implement the forty recommendations of the Summit of Lyon, in order to combat transnational organized criminal activity posing an ever-greater threat to the individual and collective security of our citizens. With increased international movement by organized criminal groups and their use of new global communications technologies, the protection of our citizens' safety, traditionally a domestic concern, requires unprecedented levels of international cooperation. Our responsibility is not only to react to the activities of organized criminal groups, but also to anticipate and prevent their growth.

We meet today at the Ministerial level to agree upon a program of specific actions designed to accomplish two critical tasks: enhancing our abilities to investigate and prosecute high-tech crimes and strengthening international legal regimes for extradition and mutual legal assistance to ensure that no criminal receives safe haven anywhere in the world.

With regard to high-tech crime, we must start by recognizing that new computer and telecommunications technologies offer unprecedented opportunities for global communication. As nations become increasingly reliant upon these technologies, including wireless communications, their exploitation by high-tech criminals poses an ever-greater threat to public safety. This threat takes at least two forms. First, sophisticated criminals are targeting computer and telecommunications systems to obtain or alter valuable information without authority and may attempt to disrupt critical commercial and public systems. Second, criminals, including members of organized crime groups and terrorists, are using these new technologies to facilitate traditional offenses. Clearly, the misuse of information systems in these ways poses a serious threat to public safety.

National laws apply to the Internet and other global networks. But while the enactment and enforcement of criminal laws have been, and remain, a national responsibility, the nature of modern communications networks makes it impossible for any country acting alone to address this emerging high-tech crime problem. A common approach addressing the unique, borderless nature of global networks is needed and must have several distinct components.

Each country must have in place domestic laws that ensure that the improper use of computer networks is appropriately criminalized and that evidence of high-tech crimes can be preserved and collected in a timely fashion. Countries must also ensure that a sufficient number of technically-literate, appropriately-equipped personnel are available to address high-tech crimes.

Such domestic efforts must be complemented by a new level of international cooperation, especially since global networks facilitate the commission of transborder offenses. Therefore, consistent with principles of sovereignty and the protection of human rights, democratic freedoms and privacy, nations must be able to collect and exchange information internationally, especially within the short time frame so often required when investigating international high-tech crimes.

The development of effective solutions will also require unprecedented cooperation between government and industry. It is the industrial sector that is designing, deploying and maintaining these global networks and is primarily responsible for the development of technical standards. Thus, it is incumbent on the industrial sector to play its part in developing and distributing secure systems that, when accompanied by adherence to good computer and personnel security practices, serve to prevent computer abuse. Such systems should also be designed to help detect computer abuse, preserve electronic evidence, and assist in ascertaining the location and identity of criminals.

To meet the challenges of the information age, we have agreed to ten Principles and a ten-point Action Plan, annexed to this Communiqué. We direct our experts to promote these Principles throughout the international community and take forward the Action Plan without delay.

Another core area of concern is mutual legal assistance and extradition. We reiterate the fundamental importance of either returning our nationals for trial in the country in which the crime was committed or, where that is not possible, conducting effective domestic prosecutions in lieu thereof. Those of us that conduct domestic prosecution of our nationals in lieu of extradition agree to pursue such prosecutions with the same commitment of time, personnel and financial resources as are devoted to the

prosecution of serious crimes committed within our own territory.

We recognize that the need for enhanced cooperation in extradition and mutual assistance is particularly acute with respect to high-tech crime and other areas of emerging significance. We commit to remove impediments in existing cooperation regimes by such means as approaching issues of dual criminality with flexibility, and we will ensure that serious computer abuses have criminal penalties sufficient to make them extraditable. We also commit to enhance coordination among States in multi-jurisdictional cases, so as to minimize conflicts and duplications in investigations and prosecutions, consult as to where best to prosecute, and allocate responsibility for gathering and sharing evidence.

We are also convinced that we must further enhance our abilities to obtain testimony from witnesses located abroad for use in criminal proceedings in our States. We agree to intensify our efforts to use video-link technology as a means of securing testimony or statements from a witness located abroad. Where possible, we will locate or establish facilities with technical video-link capability, allow the use of video-link as a form of mutual assistance to other States and provide for the punishment of perjury committed during video-link transmissions.

We emphasize that these agreed-upon cooperation measures can be used by all countries to enhance international cooperation in combating transnational organized crime. Our experts will review annually our implementation at the national level of these international legal cooperation measures. We also urge all States to adopt the recommendations of the Summit of Lyon pertaining to international legal cooperation and the best practices agreed upon by our experts to implement them.

We direct our experts to focus their future work on the following areas: Continued examination of the use of video-link technology and confiscation and sharing of assets obtained through criminal activity; identification of additional measures that would enhance cooperation in areas of emerging significance; ways to further promote acceptance by other members of the international community of the principles set forth in the above recommendations and practical actions; and coordination among The Eight on the possible elaboration of a U.N. organized crime convention.

In addition to taking action on high-tech crime and mutual legal assistance, we further direct our experts to pursue their work in implementing comprehensive action against transnational organized crime, as mandated by the Denver Summit. Therefore, we welcome the continued efforts of our experts to develop cooperative strategies and policies to combat major transnational criminal organizations and to implement joint operational projects to target such organizations and their criminal activities. We will continue to work together to combat international firearms trafficking and other forms of cross-border crime and smuggling and to address the financial aspects of organized crime.

In conclusion, we recognize the urgent need to make rapid progress in these areas and will take the steps necessary to ensure protection from the physical and financial predation of transnational organized crime. Our task is daunting, but we expect to report substantial progress in this endeavor to the Birmingham Summit in May of 1998.

COMMUNIQUÉ ANNEX:

Principles and Action Plan to Combat High-Tech Crime

Statement of Principles

We hereby endorse the following PRINCIPLES, which should be supported by all countries:

1. There must be no safe havens for those who abuse information technologies.
2. Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred.
3. Law enforcement personnel must be trained and equipped to address high-tech crimes.
4. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.
5. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.
6. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.
7. Transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides.
8. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.
9. To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.
10. Work in this area should be coordinated with the work of other relevant international fora to ensure against duplication of efforts.

Action Plan

In support of these PRINCIPLES, we are directing our officials to:

1. Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty-four hour basis.
2. Take appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other States.
3. Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.
4. Consider issues raised by high-tech crimes, where relevant, when negotiating mutual assistance agreements or arrangements.
5. Continue to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance; transborder searches; and computer searches of data where the location of that data is unknown.
6. Develop expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and to study ways to expedite the passing of this data internationally.
7. Work jointly with industry to ensure that new technologies facilitate our effort to combat high-tech crime by preserving and collecting critical evidence.
8. Ensure that we can, in urgent and appropriate cases, accept and respond to mutual assistance requests relating to high-tech crime by expedited but reliable means of communications, including voice, fax, or e-mail, with written confirmation to follow where required.
9. Encourage internationally-recognized standards-making bodies in the fields of telecommunications and information technologies to continue providing the public and private sectors with standards for reliable and secure telecommunications and data processing technologies.
10. Develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions.

Principles on Trans-Border Access to Stored Computer Data (1999)

Principles on Accessing Data Stored in a Foreign State

The G8 agree that the following principles should apply when law enforcement agents employed by law enforcement agencies are investigating criminal matters and require transborder access to, copying of, or search and seizure of electronic data (including historical traffic data, but not including interceptions), and such principles should be implemented through treaties, and through national laws and policies:

Preservation of Data Stored in a Computer System

Each State shall ensure its ability to secure rapid preservation of data that is stored in a computer system, in particular data held by third .parties such as service providers, and that is subject to short retention practices or is otherwise particularly vulnerable to loss or modification, for the purpose of seeking its access, search, copying, seizure or disclosure, and ensure that preservation is possible even if necessary only to assist another State.

A State may request another State to secure rapid preservation of data stored in a computer system located in that other State. Upon receiving a request from another State, the requested State shall take all appropriate means, in accordance with its national law, to preserve such data expeditiously. Such preservation shall be for a reasonable time to permit the making of a formal request for the access, search, copying, seizure or disclosure of such data.

Expedited Mutual Legal Assistance

Upon receiving a formal request for access, search, copying, seizure or disclosure of data, including data that has been preserved, the requested State shall, in accordance with its national law, execute the request as expeditiously as possible, by:

- Responding pursuant to traditional legal assistance procedures, or
- Ratifying or endorsing any judicial or other legal authorization that was granted in the requesting State and, pursuant to traditional legal assistance procedures, disclosing any data seized to the requesting State; or
- Using any other method of assistance permitted by the law of the requested State,

Each State shall, in appropriate circumstances, accept and respond to legal assistance requests made under these Principles by expedited but reliable means of communications, including voice, fax or email, with written confirmation to follow where required.

Transborder Access to Stored Data Not Requiring Legal Assistance

Notwithstanding anything in these Principles, a State need not obtain authorization from another State when it is acting in accordance with its national law for the purpose of:

- accessing publicly available (open source) data, regardless of where the data is geographically located
- accessing, searching, copying, or seizing data stored in a computer system located in another State, if acting in accordance with the lawful and voluntary consent of a person who has the lawful authority to disclose to it that data. The searching State should consider notifying the searched State, if such notification is permitted by national law and the data reveals a violation of criminal law or otherwise appears to be of interest to the searched State.

DATA PRESERVATION CHECKLISTS

ISSUES TO BE CONSIDERED IN A LEGAL FRAMEWORK FOR DATA PRESERVATION

Purpose: The purpose of this document is to set forth a series of questions that could be considered in any current or possible future legal framework for data preservation.

Note: For purposes of this document, the term "Preservation" shall mean that (a) upon lawful request by a competent authority, (b) based on the facts of a specific case, (c) specific ***historical*** data can be preserved to prevent its deletion, (d) pending issuance of a lawful demand from a competent authority to disclose the data. "Preservation" does not include prospective collection of data and does not obligate a service provider to generate data not already in existence.

1. Source of Law

   1.1 What is the basis in procedural law for a Preservation Order?

   1.2 Are there substantive legal predicates for is-

suance of a Preservation Order?

1.3 Are there substantive legal predicates for a Preservation Order to cover specific types of data (e.g. traffic data vs. content)?

2. Scope

What records should be subject to a Preservation Order?

3. Duration of Preservation Order

For how long should the records by pre served?

4. Form of Preservation Order

4.1 Should there be a standardized form for Preservation Orders?

4.2 Should the form of delivery for Preservation Orders be:

- Written only
- Verbal
- Verbal, followed by written confirmation
- E-mail

5. Authorized Issuers

5.1 What competent authorities ("Issuers") can issue a Preservation Order?

5.2 Should there be authentication measures to identify communications initiated by an Issuer?

6. Geographic Scope

Can a Preservation Order apply to:

6.1 Records located outside jurisdiction of Issuer?

6.2 Recipients located outside jurisdiction of Issuer?

7. Confidentiality

7.1 Can the Issuer require that the Recipient (a) maintain the confidentiality of the Preservation Order and/or (b) keep the Preservation Order confidential from the subject of the investigation?

7.2 What is the penalty for such unauthorized disclosure?

7.3 Should there be a deadline or expiration point for any confidentiality requirement?

8. Reimbursement of Recipient

Is reimbursement available to a Recipient? What costs can be recovered by the Recipient?

9. Class of Recipients

9.1 What entities ("Recipients") can be served with a Preservation Order?

9.2 What individuals or departments within a Recipient entity should receive the Preservation Order?

9.3 Can a single Preservation Order apply to multiple Recipients within a single jurisdiction? Can it apply to multiple Recipients in different jurisdictions within the same country?

10. Immunity of Recipient

Is immunity from legal action available to a Recipient in connection with its compliance with a lawful Preservation Order? Specifically, is this immunity:

10.1 Criminal immunity?

10.2 Civil immunity?

10.3 Foreign immunity?

11. Penalty for Non-Compliance

What penalty (if any) would be imposed on a Recipient who does not undertake an authorized Preservation Order?

12. Recipient's Right of Refusal

Under what circumstances is a Recipient justified in seeking clarification, modification, or otherwise not complying with a Preservation Order?

13. Duty to Revoke

Does the Issuer have a duty to revoke the Preservation Order when the Issuer no longer believes that a related disclosure order will follow?

14. Scope of Use

Can preserved data be disclosed and used pursuant to other legal process (e.g. civil subpoena) or is disclosure and use limited to the specific criminal investigation forming the basis for the Preservation Order?

15. Interaction with Mutual Legal Assistance Obligations

15.1 Is the Preservation Order process consistent

with the MLA process?

15.2 What criteria (if any) should be considered when deciding whether to issue a Preservation Order at the request of a foreign competent authority?

15.3 Is a Preservation Order appropriate or possible when preservation is sought by a foreign competent authority and the recipient competent authority considers that there may be no apparent dual criminality for the underlying incident under investigation?

16. Partial Disclosure

Should some form of partial disclosure be authorized or required in order to identify other potential Recipients who may possess data relevant to the investigation?

17. Potential Abuses

What practices or outcomes would be considered an abuse of the preservation process?

18. Potential Conflicting Laws

What laws may conflict with the requirements of a Preservation Order?

19. Disclosure Standards

What standards govern disclosure of data preserved pursuant to a lawful Preservation Order?

20. Dispute Resolution

What authority (court, commission, etc.) can resolve disputes relating to the validity or scope of a Preservation Order?

LAW ENFORCEMENT RECORD PRESERVATION CHECKLIST

Purpose: This checklist is intended to be used by individuals working for a competent authority, when issuance of a Preservation Order is possible, in the context of a specific criminal investigation.

Note: For purposes of this checklist, the term "Preservation" shall mean that (a) upon lawful request by a competent authority, (b) based on the facts of a specific case, (c) specific historical data can be preserved to prevent its deletion, (d) pending issuance of a lawful demand from a competent authority to disclose the data. "Preservation" does not include prospective collection of data and does not obligate a service provider to generate data not already in existence.

1. Identify Source of Preservation Request

1.1 Domestic

1.2 Foreign

2. Identify Legal Basis for Preservation Order

2.1 Law authorizing issuance of the Preservation Order

2.2 Underlying criminal offence forming basis for the Preservation Order

3. Identify Appropriateness and Extent of Preservation Order

3.1 Is the issuance of the Preservation Order, and the extent of the Order, appropriate? For example, are the Preservation Order and the records requested to be preserved (a) proportional; (b) relevant to the investigation; or (c) not unreasonably burdensome on the Recipient?

3.2 Are the records publicly available?

4. Identify What Information Law Enforcement Already Possesses

4.1 Individual's identity (e.g. name)

4.2 Account name (e.g. joe@internetmail.com)

4.3 Communication (e.g. E-mail from A to B)

4.4 File (e.g. graphic, text etc.)

5. Identify Recipient(s) of Preservation Order

5.1 What entity ("Recipient") should receive the Preservation Order?

5.2 What department or individual within the Recipient entity should receive a copy of the Preservation Order?

6. Identify Records to be Preserved

The following types of records may be available from a typical Internet service. It should be noted that not all of the following types of data elements will be available from every Recipient, and that actual records available will depend upon the Recipient's business model and record retention practices.

6.1 Subscriber Records (e.g. subscriber name, physical address)

6.2 Traffic Data (e.g. Userid, assigned IP address) Note: The Council of Europe Cybercrime Convention contains a definition of Traffic Data.

6.3 Stored Content (e.g. stored E-mail, stored

FTP files)

6.4 Other Relevant Information

7. Define Scope of Preservation Order

7.1 Time Period for Preservation by Recipient

7.2 Time Span for Relevant Records

8. Reimbursement for Recipient

Are there any laws, policies, or arrangements for the reimbursement of costs?

9. Identify Proper Means for Service of Preservation Order on Recipient

9.1 Written

9.2 Verbal

9.3 Verbal, followed by written confirmation

9.4 E-mail

Prepare Follow-up Plan to Obtain Disclosure

Principles on the Availability of Public Data Essential to Protecting Public Safety (2002)

To investigate, so as to prevent or prosecute, crimes and terrorist activities, law enforcement authorities require lawful access to traffic data and subscriber information held by communications service providers. However, criminal and terrorist investigations are increasingly being hampered by a lack of available data and information.

For this reason States should examine their policies concerning the availability of traffic data and subscriber information so that a balance is struck between the protection of privacy, industry's considerations and law enforcement's fulfillment of the public safety mandate. Specifically, in developing a balanced approach, States should uphold human rights, including the protection of personal data.

Data protection policies should strike a balance between the protection of personal data, industry's considerations such as network security and fraud prevention, and law enforcement's needs to conduct investigations to combat crime and terrorist activities.

Governments and industry should recognize that the advancement of technology and electronic commerce includes the safety of the public in its use. Ensuring that the public and businesses are safe and secure is essential for the continued health of national economies and the growth of consumer confidence in doing business on the Internet.

In order to facilitate a balanced approach when developing policies regarding the availability of traffic data and subscriber information, consultations should be conducted with all relevant stakeholders including data protection and privacy authorities, industry, law enforcement agencies and users.

Governments and industry should recognize that there are economic implications to the collection and retention of data, which are dependent on a number of factors including the amount of available data (e.g., which fields in which logs), the time period for storage, and different business modules. Therefore, governments should specify the types of data that would be useful for public safety purposes. Some logs, for example network access logs, are particularly useful for lawful investigations. Annex A contains a list of logs that may be available.

Governments should seek to avoid unreasonable operational and financial burdens on different ISP business models with respect to ensuring the availability of traffic data and subscriber information.

States should develop cooperative approaches regarding the availability of data in order to avoid undue burden on service providers that supply services across borders, taking into account any applicable international trade obligations.

Policies developed at the domestic level regarding the availability of traffic data and subscriber information should take into account the need for international cooperation to enable the rapid tracing of criminal and terrorist networked communications across national borders.

The following is a list of log details related to some services that may be available to an Internet service provider. It should be noted that the content of these logs might be subject to relevant business, technical and legal conditions; not all of the following data elements will be available in all logs.

1. Network Access Systems (NAS)
    - access logs specific to authentication and authorization servers such as TACAS+ or RADIUS (Remote Authentication Dial in User Service) used to control access to IP routers or network access servers
        - date and time of connection of client to server[1]
        - userid
        - assigned IP address
        - NAS IP address
        - number of bytes transmitted and received
        - Caller Line Identification (CLI[2]).
2. E-mail servers
    - SMTP (Simple Mail Transfer Protocol) log
        - date and time of connection of client to server

1 Reliable time records among different computers and networks is essential for investigation and prosecution. The use of the Network Time Protocol (NTP) for synchronization should be an ISP Best Practice

2 CLI provides the number from which a telephone call is made and may or may not be available to ISPs. CLI retrieval is specific to the given combination of software and hardware. See "LINX Best Current Practice - Traceability", section 10.2.

- IP address of sending computer
- ID Message (msgid)
- sender (login@domain)
- receiver (login@domain)
- status indicator

- POP (Post Office Protocol) log or IMAP (Internet Message Access Protocol) log
  - date and time of connection of client to server
  - IP address of client connected to server
  - userid
  - In some cases identifying information of E-mail retrieved

3. File upload and download servers
   - FTP (File Transfer Protocol) log
     - date and time of connection of client to server
     - IP source address
     - userid
     - path and filename of data object uploaded or downloaded
4. Web servers
   - HTTP (HyperText Transfer Protocol) log
     - date and time of connection of client to server
     - IP source address
     - operation (i.e., GET command)
     - path of the operation (to retrieve html page or image file)
     - "last visited page"
     - response codes
5. Usenet
   - NNTP (Network News Transfer Protocol) log
     - date and time of connection of client to server
     - protocol process ID (nnrpd[NNN……N])
     - hostname (DNS name of assigned dynamic IP address)
     - basic client activity (no content)
     - posted message ID
6. Internet Relay Chat
   - IRC log
     - date and time of connection of client to server
     - duration of session
     - nickname used during IRC connection
     - hostname and/or IP address

Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations (2002)

Governments should consider the following measures, which enhance the ability of law enforcement agencies to prevent and investigate terrorism and other criminal acts:

1. Allow service providers to retain identified categories of traffic data and/or subscriber data for legitimate business or public safety purposes, perhaps by supporting the adoption of best practice codes by service providers and service provider associations.[3]
2. Ensure data protection legislation, as implemented, takes into account public safety and other social values, in particular by allowing retention and preservation of data important for network security requirements or law enforcement investigations or prosecutions, and particularly with respect to the Internet and other emerging technologies.
3. Permit domestic law enforcement to serve foreign preservation instructions to domestic service providers after expedited approval, with substantive review if required by domestic law, through a domestic judicial or similar order.
4. Ensure the expeditious preservation of existing traffic data regarding a specific communication whether one or more service providers were involved in its transmission, and the expeditious disclosure of a sufficient amount of traffic data to enable identification of the service providers and path through which the communication was transmitted, through the execution of a single domestic judicial or similar order where permitted by domestic law.
5. Authorize domestic law enforcement to use the mechanisms described in the prior paragraph to respond to a foreign request, through expedited mutual assistance, even if there is no violation of the domestic law of the requested State.[4]
6. Upon receiving a request from another State to trace a specific communication, authorize competent authorities, even if there is no violation of the domestic law of the requested State, to use mechanisms available under domestic law expeditiously to preserve all existing domestic data necessary to trace the communication, notify the requesting State if the communication appears to come from a third State, and provide sufficient data to the requesting State so that it may request assistance from the third State.
7. Authorize domestic law enforcement to trace in real-time specified communications in order to determine their path, origin or destination, including through multiple providers in a country, using a single domestic judicial or similar order if permitted under domestic law.
8. Authorize domestic law enforcement to use the mechanisms described in the prior paragraph to respond to a foreign request, through expedited mutual assistance, even if there is no violation of the domestic law of the requested State.
9. Encourage network architecture that improves security and allows, in appropriate cases, tracing of network abuses with due regard for the privacy of network users.
10. Encourage strong user-level authentication for appropriate applications, with due regard for technological neutrality and users' freedom of choice.

3 The category or categories of data would be determined by each State.

4 The phrase "even if there is no violation of the domestic law of the requested State" is intended to signify that the requested State should provide assistance even if the conduct at issue does not meet all the conditions to qualify as a crime or cannot otherwise by prosecuted as a crime in that State. The phrase and these Recommendations generally, are not intended to limit the possible imposition of other requirements for providing assistance that may be imposed by a requested State, including dual criminality requirements or exceptions for the essential interests of the requested State.

Principles for Protecting Critical Information Infrastructure (2003)

Information infrastructures form an essential part of critical infrastructures. In order effectively to protect critical infrastructures, therefore, countries must protect critical information infrastructures from damage and secure them against attack. Effective critical infrastructure protection includes identifying threats to and reducing the vulnerability of such infrastructures to damage or attack, minimizing damage and recovery time in the event that damage or attack occurs, and identifying the cause of damage or the source of attack for analysis by experts and/or investigation by law enforcement. Effective protection also requires communication, coordination, and cooperation nationally and internationally among all stakeholders – industry, academia, the private sector, and government entities, including infrastructure protection and law enforcement agencies. Such efforts should be undertaken with due regard for the security of information and applicable law concerning mutual legal assistance and privacy protection. To further these goals, we adopt the following PRINCIPLES and encourage countries to consider them in developing a strategy for reducing risks to critical information infrastructures:

1. Countries should have emergency warning networks regarding cyber vulnerabilities, threats, and incidents.
2. Countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them.
3. Countries should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures.
4. Countries should promote partnerships among stakeholders, both public and private, to share and analyze critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures.
5. Countries should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.
6. Countries should ensure that data availability policies take into account the need to protect critical information infrastructures.
7. Countries should facilitate tracing attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other countries.
8. Countries should conduct training and exercises to enhance their response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack and should encourage stakeholders to engage in similar activities.
9. Countries should ensure that they have adequate substantive and procedural laws, such as those outlined in the Council of Europe Cybercrime Convention of 23 November 2001, and trained personnel to enable them to investigate and prosecute attacks on critical information infrastructures, and to coordinate such investigations with other countries as appropriate.
10. Countries should engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analyzing information regarding vulnerabilities, threats, and incidents, and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.
11. Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.

Best Practices for Network Security, Incident Response and Reporting to Law Enforcement (2004)

BEFORE CONFRONTING A COMPUTER INCIDENT:

1. *Be Familiar With Established Procedures, Practices, and Points of Contact.* Your organization should have procedures in place to handle computer incidents. Find these procedures, review them, and make them available to all personnel who have system security responsibilities. The procedures should provide specific guidance for you to follow. Procedures should specify: who in your organization has lead responsibility for internal incident response; who is the point-of-contact for inside and outside contacts; who inside and outside the organization requires immediate notification; and at which point law enforcement should be notified. If your organization does not have such plans, do not wait until an incident to start developing them.

   Also, determine and review which logs, if any, your system routinely captures and stores, and the period for which they are stored, and see if this practice is most suitable and appropriate to your needs.

   Finally, some legal systems will allow real-time monitoring of attacks if prior notice of this monitoring is given to all users. For this reason, consider deploying written warnings, or "banners," on the ports through which an intruder is likely to access your organization's system and on which you may attempt to monitor a hacker's communications and traffic. If you already have banners in place, review them to ensure that they are appropriate for the type of monitoring you anticipate conducting in response to a cyber-attack.

WHILE RESPONDING TO A COMPUTER INCIDENT:

2. *Make Initial Identification and Assessment of Incident.* Make an initial identification of the type of incident, and take steps to confirm that it is, in fact, an incident. Using network topology and trusted relationships, determine how many and which systems were affected, and I which way(s) they were affected, even if it is not readily apparent that certain systems have been affected. Good indicators will include evidence that files or logs were accessed, created, modified, deleted or copied, or that user accounts or permissions have been added or altered. In the case of a root-level intrusion, watch carefully for any signs that the intruder is in multiple areas of your system and possibly still undetected. Using your log information, attempt to determine (a) the immediate origin of the attack; (b) the identity of servers to which the data were sent (if information was transferred); and (c) the identity of any other victims. Remember, an intruder may have installed several paths into your organization's system, some of which you may not have discovered, some of which you may not be able to discover until you have engaged in painstaking analysis, and some of which you may never discover.

   Initial identification and assessment may not be an easy task; a system may have been Trojanized in such a way that it is difficult to detect certain file or configuration changes. Since it is likely that you will not know all of the implications of a particular incident when first detected, it is also likely that you will not know the extent to which other systems have been affected. Take care to ensure that any actions you undertake do not modify system operations or stored data in a way that could compromise your response.

3. *Take Steps to Minimize Continuing Damage.* You may need to take certain steps to stop continuing damage from an ongoing assault on your organization's network, such as installing filters to block a denial-of-service attack, or isolating all or parts of your system. In the case of unauthorized access or access that exceeds user authorization, you may decide either to block further illegal access or to watch the illegal activity in order to identify the source of the attack and/or learn the scope of the compromise.

   In reviewing your options, consider that (at least in the case of a remote intruder) isolating the network from other networks and cutting off outside access may alert the attacker that you have seen his activity and thereby eliminate any chance of identifying the attacker. Further, if your attempt to cut off access is detected but ineffective, the attacker may inflict damage in retribution or take other steps to destroy evidence or otherwise hide his activities. If you do decide to block access to the intruder, install all appropriate system patches that address known vulnerabilities, look for and remove any back-doors or Trojanized programs, and watch

your organization's system vigilantly. Alternatively, you may decide to maintain overall outside connectivity but isolate (or segment-off) particularly infected systems from the remaining network and/or the Internet.

Consult with others in your organization to determine if disconnecting the network is feasible and appropriate as a business and legal matter. Also consult to determine the best technical method for proceeding.

Remember to keep detailed records of the costs imposed on your organization as a result of steps taken to mitigate the damage flowing from the attack, and keep records of the specific processes used to mitigate the attack. Such information may be important for recovery of damages from responsible parties and for any subsequent criminal investigation.

4. *Do Not Hack Into or Damage Source Computer.* Although you may be tempted to do so (especially if the attack is ongoing), do not take offensive measures on your own, such as "hacking back" into the attacker's computer.

Doing so may be illegal, regardless of the motive. As most attacks are launched from compromised systems of unwitting third parties, "hacking back" can damage the system of an innocent party. If appropriate, however, you can contact the system administrator from the attacking computer to request assistance in stopping the attack or in determining the source of the attack.

5. *Record and Collect Information.*

A. Consider Making a Complete Copy (a "Mirrored Image") of the Affected Systems. Consider making an immediate identical copy of the affected system, which will preserve a record of the system at the time of the incident for later analysis. This can be particularly helpful if an incident occurs before your organization has procedures in place. In many instances, mirrored backups prove invaluable in later attempts to identify vulnerabilities exploited, data removed, and sniffers installed, as well as to aid efforts to track the attacker. In addition, locate and obtain previously generated backup files.

Bit-by-bit and file-by-file backups both have advantages and disadvantages. Bit-by-bit copies will capture hidden files and directories, swap data, deleted data and information in slack space, all of which may provide critical clues for an investigator. However, bit-by-bit copying may be overly burdensome or otherwise impractical, necessitating more efficient methods of file or system-wide back-up.

New or sanitized media, which is subsequently protected from alteration should be used to store copies of any data which is retrieved and stored, and access to this media should be controlled, in order to maintain the integrity of the copy's authenticity, to keep undetected insiders away from it, and to help establish the chain of custody of any media.

These steps will enhance the value of any backups as evidence in any later internal investigations, civil suits or criminal prosecutions.

B. Make Notes / Keep Records / Preserve Data. As the investigation progresses, information that was collected at earlier stages of the investigation may have great significance. You should take immediate steps to preserve relevant logs that already exist and you should keep an ongoing written record of all steps undertaken so that you will not need to rely on your memory and the memory of others. The types of information that you should try to record include:

- A description of all incident-related events;
- Dates and times (and time zone, preferably in GMT) when incident-related events were discovered or occurred;
- Information (names, dates, times) concerning incident-related phone calls, e-mails and other contacts;
- Identity of persons working on incident-related tasks, a description of those tasks and amount of time spent on tasks;
- Identity of the systems, accounts, services, data and networks affected by the incident, and how these network components were affected; and
- Information relating to the amount and type of damage inflicted by the incident, which can be important if your organization decides to take action to recover these costs from responsible parties or if prosecution of responsible parties is undertaken.

Include in these records copies of all audit information (e.g., system log files and root history files), and secure process/status information and suspicious files. Remember that logs may be in several locations (e.g., logs may be stored locally as well as with a centralized syslog host);

get as many as possible. Time and date information in logs will be very important in tracing an attacker and, later, in proving his responsibility if he is caught. Therefore, be sure that log entries accurately reflect this information. Because logs may be stored on servers in various time zones, take care to identify the respective time zone for each log.

As mentioned above, keep information you record and collect in a location and on a medium which cannot easily be altered or destroyed by others. For this reason, you may want to keep handwritten notes and print out all logs, instead of keeping them in a digital format.

Designate one person to be responsible for maintaining control and possession of any records, logs, and backup files. It may be important at a later date to establish the chain of custody of these records in order to show that the records have not been altered. ("Chain of custody" refers to the means by which evidence was handled from the time of collection to the time it is used as evidence in a judicial proceeding, and to the identities of all individuals who had access to this evidence.) Usually, it is easier to show a secure chain of custody if only one person is needed to testify about the storage of the data.

C. Make Sure You Record and Log Continuing Attacks. When an attack is on-going or when your system has been infected by a virus or worm, make sure you are recording or logging this continuing activity. If you were not logging, begin immediately. Logging can be done both on a system or on an affected server; decide which is better.

You may be able to use a "sniffer" or other monitoring device to record communications between the intruder and any server that is under attack. Such activity usually is permissible if it is done to protect the rights and property of the system under attack, if a user consents to such monitoring, or if you obtain implied consent from the intruder (e.g., by means of notice or a "banner"). Where monitoring is permissible with explicit or implied consent, determine if your system has deployed banners on the ports through which the intruder is accessing your organization's system and on which you intend to monitor the traffic. (Warning banners can be a useful method to obtain implied consent to monitor from authorized and unauthorized users.) A banner should notify users or intruders as they access or log into the system that their use of the system constitutes their consent to monitoring and the results of monitoring may be disclosed to law enforcement and others. (Bannering a high-numbered or unusual port through which the intruder is entering the system may be difficult; likewise, a banner may also put the intruder on notice that he is being observed.)

Consult with your organization's legal counsel to make sure such monitoring is consistent with employment agreements, privacy policies, and legal authorities and obligations in your country, and to receive guidance with respect to the deployment of banners.

6. *Share Information*

A. Do Not Use Compromised System(s) to Communicate About Incident. Do not use a system that you suspect has been compromised to communicate about an incident or to discuss incident response. If the system has been compromised, using the system to discuss incident handling may compromise the investigation and thwart chances to block or catch the culprit. Preferably, use out-of-band modes to communicate, such as telephones and fax machines. If you must use the compromised system to communicate, encrypt all relevant communications. To avoid being the victim of social engineering and risking further damage to your organization's network, do not disclose incident-specific information to callers who are not known points-of-contact, unless you can verify the identity and authority of those persons. Treat suspicious calls, e-mails and other attempts to get information as part of the incident investigation.

B. Notify Appropriate People in Your Organization. Let appropriate people in your organization know immediately about the incident and any results of your preliminary investigation. This may include security coordinators, managers and legal counsel. (Your written policy for incident response should set out points of contact within your organization; thresholds for contacting them will be extremely useful.) When making these contacts, use only protected or reliable channels of communication. If you suspect that the perpetrator of an attack is an insider, or may have insider information, you may wish to strictly limit incident information to a need-to-know basis.

C. Contact Appropriate Computer Incident-Reporting Organization or CERT. Contacting an incident-reporting organization, such as a CERT,

to report the incident and identify the means of attack may help to prevent the attack from happening again and may prevent the attacker from finding other targets. This not only helps protect your system from further damage; it also helps to alert other actual or potential victims who otherwise might not be aware of the suspect activity.

D. Consider Notifying Other Victims or Vendors. If you learn of another victim, or you learn of a vulnerability in a vendor's product which is being exploited, you may want to notify the victim or vendor or see that an incident-reporting organization or CERT alerts the victim or vendor. They may be able to provide information about the incident of which you are not aware (e.g., hidden code, ongoing investigations in other areas, network configuration techniques). In addition, you may be able to prevent further damage to other systems.

E. Report Criminal Activity to Law Enforcement. If, at any point during your response or investigation, you suspect that the incident constitutes criminal activity, contact law enforcement immediately. Some indications that the incident involves criminal conduct include:

- An unauthorized user logged into or using the system;
- Abnormal processes running on the system which use abnormally high amounts of system resources;
- A virus or worm infecting the system;
- A user from a remote site trying to penetrate the system through unusual means of access, such as through a high-numbered port or suspicious port scanning; and
- A heavy volume of packets reaching the system in a short period of time (from the same or varied sources).

If you see such activity, follow the procedures you have in place, which may direct you to contact your organization's attorney, local law enforcement, or other criminal investigative entity. To the extent permitted by law, share the information you have gathered with law enforcement. Based on the technical nature of these investigations, many law enforcement agencies have limited capabilities in the area of cybercrime investigations. Therefore, prior contact with the various law enforcement agencies in your area is recommended to identify a technically-proficient point of contact. If you have a prior relationship with law enforcement in your area, the transfer of information can occur more quickly and efficiently. Explain to your law enforcement contact any confidentiality concerns and potential disruptions to business that may occur due to law enforcement activities.

Although, as system administrator, you may take certain steps to protect your organization's system, you should consult with legal counsel to determine what information you may collect and disclose to law enforcement and any other steps you may take to aid in a criminal investigation – both with and in the absence of legal processes.

Law enforcement has legal tools that are typically unavailable to victims of attack, and these tools can greatly increase the chances of identifying and apprehending the attacker. For example, law enforcement often can require upstream and downstream providers to preserve transactional logs and other evidence, can seek court orders or other legal means to require disclosure of those logs and other evidence, can search and seize evidence, and can require electronic surveillance.

When law enforcement arrests and successfully prosecutes an intruder, that intruder is deterred from future assaults on the victim. This is a result that technical fixes to the network cannot duplicate with the same effectiveness. Intrusion victims may try to block out an intruder by fixing the exploited vulnerability, only to find that the intruder has built in a back door and is able to continue to access the system. Catching and prosecuting the intruder may be the only method to truly secure your organization's system from future attacks by the culprit. In addition, by using the criminal justice system to punish the intruder, other would-be hackers may be deterred from attacking your organization's networks. Criminal law enforcement can thus play a significant and long-term role in network security.

AFTER A COMPUTER INCIDENT:

7. *Take Steps to Prevent Similar Attacks from Happening Again.* In order to keep similar incidents from occurring, do an "after action" report, i.e., a post-incident review of your organization's response to the attack and assessment of the strengths and weaknesses of this response. Also, be familiar with ongoing risk assessments made by your organization and by outside experts.

Best Practices for Law Enforcement Interaction with Victim-Companies During a Cyber-Crime Investigation (2005)

When conducting a cybercrime investigation involving a victim-company, law enforcement should consider the measures outlined below, while being mindful that victim-companies may themselves be involved in related criminality. These procedures are intended to:

a. Improve the likelihood of conducting a successful investigation by helping to establish a trusted relationship with victim-companies, thereby improving the quality of cooperation provided by victim-companies;

b. Help investigators to better safeguard victim-companies by reducing the likelihood that an investigation will exacerbate the damage already suffered by victim-companies; and

c. Help law enforcement establish procedures for obtaining efficient and timely assistance from victim-companies.

1. *Minimize the disruption to a victim-company's normal business operations.* Law enforcement should weigh countervailing considerations as it plans to implement investigative measures that may disrupt business operations. Where there is a choice between disruptive investigative measures and equally effective, less disruptive measures, law enforcement should always opt for the latter. Law enforcement should make every effort to use investigative measures that minimize computer downtime and displacement of a victim-company's employees. While some investigative measures that may inconvenience a victim-company are unavoidable, some less important measures may needlessly aggravate or prolong the damage already suffered by a victim-company. For example, rather than seizing compromised computers and depriving a victim-company of their use, law enforcement should consider creating a "mirror image" of the system or part of the system and leaving the original computers in place.

2. *Coordinate the release of any information to the news media about the investigation.* Investigations and prosecutions of cybercrime cases may entail the voluntary release of information to the news media by law enforcement (e.g., in a press release or at a press conference). Where possible, public statements to the news media should be coordinated with victim-companies where information that is potentially harmful to that victim-company may be released. Of course, law enforcement and justice officials should take all possible measures to prevent unauthorized releases of information about a pending investigation and to seek sanctions against those who make unauthorized disclosures.

3. *Work closely with victim-companies on issues that will have an impact on sentencing.* In many instances, it will be important to quantify the damage suffered by the victim-company as a result of a cybercrime. An accurate assessment of damages may be needed to satisfy the legal elements of an offense or to ensure that the punishment meted out at sentencing adequately reflects the damage suffered by the victim-company. It will be difficult to obtain a realistic assessment of the damage caused to a business and its productivity and to quantify the company's costs of remediating the damage without receiving significant assistance from the victim-company.

4. *To the extent possible, regularly update the victim-company on the progress of the investigation.* After the initial onsite investigation is conducted, law enforcement may have little direct contact with a victim-company. To the extent possible (and without jeopardizing any aspect of the investigation), law enforcement should inform victim-companies of the general progress of the investigation. If an arrest is made that results in court proceedings, notify the victim-company of all significant court dates, so it has the opportunity to attend.

5. *Consult with the victim-company's information technology staff about network architecture before implementing investigative measures on the network.* It is difficult to implement some investigative measures on a victim-company's network without first consulting with individuals in the company who are knowledgeable about the architecture of the company's network. It is usually advantageous to work closely with the information technology staff at a victim-company to obtain critical information about network topology, the type and version of software being run on the network, and any vagaries of the network, in order to minimize disruption of or damage to the company's network. Be mindful, however, that victim-companies can themselves be involved in the criminality un-

der investigation; before government officials coordinate investigative activities with a victim-company, they should have confidence that the company is not a culpable party.

6. *Be aware that you may need to consult with a victim-company's senior management before undertaking intrusive investigative measures on the company's network.* It is not always apparent who within a company has the authority to make binding commitments to law enforcement or to consent on behalf of the company to investigative measures that will affect the operation of the company's network. Law enforcement will often deal directly with a company's system administrator following a report of a cybercrime incident. However, system administrators may lack the authority to give the company's consent to law enforcement activity on the company's network that will affect business operations. Be aware that some decisions may require the authorization of a company's senior management and be prepared to consult with the appropriate persons at the appropriate level within the company's management structure.

7. *Encourage ongoing relationships with businesses before an incident occurs.* While a strong working relationship can be built between a victim-company and investigators during the course of a cybercrime investigation, it is preferable to have already established a relationship with a company before it is the victim of a cybercrime. Many companies are reluctant to report cybercrime incidents to law enforcement because they are fearful that law enforcement will conduct an investigation in a manner harmful to their business interests or because they have misconceptions about how law enforcement will conduct an investigation. Such fears and misconceptions can more easily be dispelled if law enforcement has a pre-existing relationship with a victim-company. For example, conducting presentations for trade associations on investigative procedures or forming liaison groups comprised of law enforcement and private industry representatives can help bridge the gap of mistrust or unfamiliarity and increase cybercrime reporting by private industry.

INTERNATIONAL TELECOMMUNICATION UNION

Resolution on Non-Discriminatory Access and Use of Internet Resources (2008)

The World Telecommunication Standardization Assembly (Johannesburg, 2008),

Considering that one of the purposes of ITU laid down in Article 1 of the ITU Constitution is "to maintain and extend international cooperation among all its Member States for the improvement and rational use of telecommunications of all kinds",

Considering further approved documents of the World Summit on the Information Society (WSIS), Geneva 2003 and Tunis 2005, in its Declaration of Principles, especially § § 11, 19, 20, 21 and 49 thereof,

Noting that § 48 of the WSIS Declaration of Principles recognized that: "The Internet has evolved into a global facility available to the public and its governance should constitute a core issue of the Information Society agenda. The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism",

Recognizing a) that the second phase of WSIS (Tunis, November 2005) identified ITU as the possible moderator/facilitator for the following WSIS Action Lines from the Plan of Action: C2 (Information and communication infrastructure) and C5 (Building confidence and security in use of the ICTs); b) that the Plenipotentiary Conference (Antalya, 2006) entrusted the ITU Telecommunication Standardization Sector (ITU-T) with a range of activities aimed at implementing the WSIS (Tunis, 2005) outcomes, a number of those activities having to do with Internet-related issues; c) Resolution 102 (Rev. Antalya, 2006) of the Plenipotentiary Conference on ITU's role with regard to international public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses; d) that management of the registration and allocation of Internet domain names and addresses must fully reflect the geographical nature of the Internet, taking into account an equitable balance of interests of all stakeholders,

Taking into account a) that ITU-T is dealing with technical and policy issues related to IP-based networks, including the Internet and next-generation networks; b) that a number of the resolutions of this assembly deal with Internet-related issues,

Resolves to invite Member States

1. to refrain from taking any unilateral and/or discriminatory actions that could impede another Member State from accessing public Internet sites, within the spirit of Article 1 of the Constitution and the WSIS principles;
2. to report to the Director of the Telecommunication Standardization Bureau on any incident referred to in 1 above,

Instructs the Director of the Telecommunication Standardization Bureau

1. to integrate and analyse the information on incidents reported from Member States;
2. to report this information to Member States, through an appropriate mechanism,

Invites Member States and Sector Members to submit contributions to the ITU-T study groups that contribute to the prevention and avoidance of such practices.

Sample Legislative Language for Cyber Crime

Preamble

This Law is necessary and based upon the common understanding of this country and the global community of nation states that the security and economic well being of all is dependent upon a harmonized global framework that counters cybercrime. Therefore:

Having regard to UN General Assembly Resolutions 45/121, 55/63, 56/121, 57/239, and 58/199 with respect to countering cybercrimes and the misuse of computers and creating cultures of security, and with respect to the extensive work advancing cyber security that has been performed by numerous multilateral organizations, such as the Organization for Economic Cooperation and Development, the Asia-Pacific Economic Cooperation forum, the Group of Eight, and the Council of Europe, with particular regard to the Convention on Cybercrime;

Believing that globalization and the use of cyberspace continues to spawn both positive and negative social impacts, resulting in legitimate trade and criminal activities that co-exist in the same network commons;

Realizing that positive impacts of the Internet and ICTs include a limitless possibility for improving human conditions in this and all nations by providing new mechanisms for education, facilitating global trade, meeting the basic needs of people, improving communication and health care, enabling economic benefits, and offering opportunities for upward mobility to underserved populations;

Acknowledging the negative impacts of global connectivity – such as interference with networks and data, theft and/or disclosure of private or protected information, fraud, identity theft, money laundering, phishing, spam, and disruptions to critical infrastructure or cyber warfare – work to prevent many from participating in or realizing the full benefits of the new global community;

Admitting that resources for addressing the problem of cybercrime and assuring the safety and security of networks vary within enterprises and across nations, and that even in the best of circumstances, system administrators are overtaxed and under-prepared to deal with the continuous barrage and evolution of threats;

Understanding that deterring cybercrime is necessary to enabling the benefits of cyberspace for the global population, and that such deterrence requires international cooperation, information sharing, and investigative assistance among all nations and global harmony in legal systems;

Considering that it is necessary to define the behaviors, actions, and activities that can be consistently described as unacceptable, along with the procedures to be followed when these behaviors are observed or investigated;

Realizing that the ability to effectively prosecute cyber criminals—and cyber terrorists—requires common approaches to the criminality of such acts as well as consistency with respect to jurisdictional issues, such as cooperation in investigations, search and seizure of digital evidence, and extradition;

Understanding that harmonizing laws will help to eliminate safe havens for attackers and establish a uniform risk to which they place themselves through their actions;

Desiring to further secure the benefits of cyberspace and a globally connected society for this country through our collaboration, cooperation, and coordination in the investigation and prosecution of cyber criminal acts that occur domestically and across international borders;

Acknowledging that cyberspace requires a framework that can adapt and extend existing legal responses that have been effective in deterring crimes committed offline into the realm of cyberspace; in other cases, new rules must address crimes that have no existing offline counterpart, and thus require a completely new legislative effort;

Concluding that this Law is required in order to enable the people of this country the opportunity to enjoy the benefits of cyberspace and to deter and to punish those who would inflict harm by the use of its networks.

TITLE 1
DEFINITIONS

Section 1
Definitions

For purposes of this Law:

(a) *Access*

Access means to make use of; to gain entry to; to view, display, instruct, or communicate with; to store data in or retrieve data from; to copy, move, add, change, or remove data; or otherwise make use of, configure, or reconfigure any resources of a computer program, computer,

computer system, network, or their accessories or components, whether in whole or in part, including the logical, arithmetical, memory, transmission, data storage, processor, or memory functions of a computer, computer system, or network, whether by physical, virtual, direct, or indirect means or by electronic, magnetic, audio, optical, or other means.

(b) *Computer*

Computer means an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping or such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device(s), but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

(c) *Computer Data*

Computer data means any representation of facts, information, concepts, elements, state, or instructions in a form suitable for communications, interpretation, or processing in a computer program or part of a program, computer, or computer system, suitable to cause a computer program, computer, computer system, or network to perform a function, process, and/or operation.

(d) *Computer Program*

Computer program means a set of coded instructions, whether in machine readable or human readable formats, that enables a computer, computer system, and/or network to process computer data, traffic data, and/or content data to cause such computer, computer system, and/or network to perform a function and/or operation.

(e) *Computer System*

Computer System means a computer, physical or virtual, or collection of such computers and any components and/or accessories, temporarily or permanently interconnected or related, and one or more of which contain computer programs, computer data, content data, and/or traffic data, in whatever form, that perform functions, including, but not limited to: logic, arithmetic, information creation, storage, sorting, copying, changing, *retrieval*, destruction, routing, communications, and/or control.

(f) *Content Data*

Content Data means any data whether in digital, optical, or other form, including metadata, that conveys essence, substance, information, meaning, purpose, intent, or intelligence, either singularly or when in a combined form, in either its unprocessed or processed form.

(g) *Critical Infrastructure*

Critical infrastructure means the computers, computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data, content data and/or traffic data so vital to this country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.

(h) *Cyberspace*

The physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks, and their computer programs, computer data, content data, traffic data, and users.

(i) *Damage*

Damage means any disruption, interception, interference, and/or destruction of computer data, content data, traffic data, a computer program, computer, computer system, or network, including the transmission and/or receipt of computer data, content data, or traffic data by a computer program, computer, computer system, or network.

(j) *Disruption*

An event that causes a computer program, computer, computer system, network, or component thereof, to be inoperable, or operate in an unintended manner, for a length of time due to destruction of and/or interference with a computer program, computer, computer system, network, computer data, content data, and/or traffic data.

(k) *Interception*

Interception means the acquisition, viewing, capture, or copying of the contents or a portion thereof, of any communication, including content data, computer data, traffic data, and/or electronic emissions thereof, whether by wire, wireless, electronic, optical, magnetic, oral, or other means, *during transmission* through the use of any electronic, mechanical, optical, wave, electromechanical, or other device.

(l) *Interference*

Interference means (i) hindering, blocking, impeding, interrupting, or impairing the processing of, functioning of, access to, or confidentiality, integrity, or availability of a computer program, computer, computer system, network, computer data, content data, or traffic data by inputting, transmitting, damaging, deleting, destroying, deteriorating, altering, or suppressing computer data, content data, traffic data, a computer program, computer, computer system, or network, and/or (ii) corrupting, damaging, deleting, deteriorating, altering, or suppressing a computer program, computer data, content data, or traffic data.

(m) *Loss*

Loss means any reasonable costs, including, but not limited to, the cost of responding to an offense under this

Law, conducting an investigation or damage assessment, and/or the cost of analyzing, restoring, replacing, or reproducing computer data, content data, traffic data, a computer program, computer, computer system, or network to its condition prior to the offense, and/or other consequential damages incurred by an individual or entity arising from damage, interference, disruption, interception and/or the destruction of computer data, content data, traffic data, a computer program, computer, computer system, network, and/or other information.

(n) *Malware*

A program that is inserted into a computer program, computer, or computer system, usually covertly or without authorization, with the intent of compromising the confidentiality, integrity, or availability of the computer program, computer, computer system, network, computer data, content data, or traffic data or of otherwise disrupting the beneficial use thereof.

(o) *Network*

A group of computers or computer systems of whatever form, topology, or functionality that is connected at points (nodes) which have the capability to transmit, receive, share, or forward information, communication signals, and operational instructions.

(p) *Service Provider*

Service provider means:

(i) any public or private entity that provides to users of its service the ability to communicate by means of a computer program, computer, computer system, or network, including the services that support the development or utilization of computer programs and/or the creation, storage, retrieval, processing, management, and deletion of computer data, traffic data, and content data; and/or

(ii) any other entity that processes or stores computer data, content data, or traffic data on behalf of such service (as set forth in (i) of this paragraph) or users of such service.

(q) *Subscriber Information*

Subscriber information means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, and by which can be established: (i) the type of communication service used, the technical provisions taken thereto, and the period of service; (ii) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, as it is available on the basis of the service agreement or arrangement; and/or (iii) any information regarding the location of installed communications equipment as disclosed in the service agreement or arrangement.

(r) *Traffic Data*

Traffic data means any computer or other data relating to a communication by means of a computer program, computer, computer system, or network, generated by a computer program, computer, computer system, or network that formed a part in the chain of communication, indicating the communication's origin, destination, route, format, intent, time, date, size, duration, or type of underlying service.

TITLE 2
SUBSTANTIVE PROVISIONS; ACTS AGAINST COMPUTERS, COMPUTER SYSTEMS, NETWORKS, COMPUTER DATA, CONTENT DATA, AND TRAFFIC DATA

Section 2
Unauthorized Access to Computers, Computer Systems, and Networks

(a) *Unauthorized Access to Computers, Computer Systems, and Networks*

Whoever knowingly accesses in whole or in part, without authorization or in excess of authorization or by infringement of security measures, (i) a computer, (ii) a computer system and/or connected system, or (iii) a network, with the intention of conducting any activity within the definition of "Access" in this Title and which is prohibited under this Law shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(b) *Unauthorized Access to Government Computers, Computer Systems, and Networks*

Whoever commits unauthorized access pursuant to paragraph (a) of this Section to a computer, computer system and/or connected system, or network that is exclusively for the use of the Government of this country, or in the case which such is not exclusively for the use of the Government but is used by or on behalf of the

Government of this country and such conduct affects that use or impacts the operations of the Government of this country, a criminal offense shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(c) *Unauthorized Access to Critical Infrastructure*

Whoever commits unauthorized access pursuant to paragraph (a) of this Section to a computer, computer system and/or connected system, or network that is exclusively for the use of critical infrastructure operations, or in the case which such is not exclusively for the use of critical infrastructure operations but the computer, computer system and/or connected system, or network is used for critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure, shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(d) *Unauthorized Access for Purposes of Terrorism*

Whoever commits unauthorized access pursuant to paragraph (a) of this Section with the intent of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to acts of cyber terrorism, shall have committed a criminal offense punishable by a fine of [amount]_____ and imprisonment for a period of _____.

Section 3
Unauthorized Access to or Acquisition of Computer Data, Content Data, Traffic Data

(a) *Unauthorized Access to or Acquisition of Computer Program, Computer Data, Content Data, Traffic Data*

Whoever knowingly accesses and/or acquires, in whole or in part, without authorization or in excess of

authorization or by infringement of security measures (i) a computer program, (ii) computer data, (iii) content data, or (iv) traffic data, with the intention of conducting any activity within the definition of "Access" in this

Title and which is prohibited under this Law shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(b) *Unauthorized Access to or Acquisition of Protected Government Computer Program or Data*

Whoever commits unauthorized access and/or acquisition pursuant to paragraph (a) of this Section with the intent to access and/or acquire a computer program, computer data, content data, or traffic data that has been determined by the Government of this country, pursuant to law or decree, to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any other reason pertaining to national or economic security, a criminal offense shall have been committed, punishable by a fine of [amount]_____ and imprisonment for a period of _____, irrespective of whether or not such program or data was communicated, delivered, or transmitted to any person not entitled to receive it or retained by the person who accessed it.

(c) *Unauthorized Access to or Acquisition of Government Computer Program or Data*

Whoever commits unauthorized access and/or acquisition pursuant to paragraph (a) of this

Section with the intent to access and/or acquire a computer program, computer data, content data, or traffic data that is used, processed, or stored by any ministry, agency, department, office, or entity of the Government of this country and such data or program is exclusively for the use of the Government of this country, or in the case in which such data or program is not exclusively for the use of the Government but it is used by or on behalf of the

Government and such conduct affects that use or impacts the operations of the Government of this country, a criminal offense shall have been committed, punishable by a fine of [amount] _____ and/or imprisonment of _____.

(d) *Unauthorized Access to or Acquisition of Critical Infrastructure Program or Data*

Whoever commits unauthorized access and/or acquisition pursuant to paragraph (a) of this Section with the intent of accessing and/or acquiring a computer program, content data, computer data, or traffic data that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but the program or data is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure, a criminal offense shall have been committed, punishable by a fine of [amount]_____ and imprisonment of _____.

(e) *Unauthorized Access to or Acquisition of Computer Programs or Data for Financial Data or Illegal Acts*

Whoever commits unauthorized access and/or acquisition pursuant to paragraph (a) of this Section with the intent of (i) accessing or acquiring financial data of a financial institution, or (ii) facilitating, advancing, assisting, conspiring, or committing extortion, identity theft, or any other illegal act not covered by provisions within this Law, whether or not via a computer program, computer, computer system, or network, a criminal offense shall have been committed, punishable by a fine of [amount]_____ and/or imprisonment of _____.

(f) *Unauthorized Access to or Acquisition of Computer Programs or Data for Purposes of Terrorism*

Whoever commits unauthorized access and/or acquisition pursuant to paragraph (a) of this Section with the intent of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to acts of cyber terrorism, a criminal offense shall have been committed, punishable by a [amount]_____ fine and imprisonment for a period of _____.

Section 4
Interference and Disruption

(a) *Interference and Disruption of Computers, Computer Systems, Networks*

Whoever, without authorization or in excess of authorization or by infringement of security measures, intentionally causes interference and/or disruption of a computer, computer system and/or connected systems,

or networks shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(b) *Interference and Disruption of Computer Program, Computer Data, Content Data, Traffic Data*

Whoever, without authorization or in excess of authorization or by infringement of security measures, intentionally causes interference and/or disruption of a computer program, computer data, content data, or traffic data shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(c) *Interference or Disruption With Knowledge of or Intent to Cause Serious Harm or Threaten Public Safety*

Whoever commits interference and/or disruption pursuant to paragraphs (a) or (b) of this Section with the intent to cause or with knowledge that such conduct could cause serious harm to life, limb, or property or threaten public health and/or safety, shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(d) *Knowledge of or Intent to Cause Interference or Disruption of Government Computers, Systems, Networks, Data*

Whoever commits interference and/or disruption pursuant to paragraphs (a) or (b) of this Section with the intent to cause or with knowledge that such conduct could cause interference and/or disruption of computers, computer systems and/or connected systems, networks, computer programs, computer data, content data, or traffic data used by the Government in furtherance of the administration of justice,

national security, or national defense shall have committed a criminal offense punishable by a fine of [amount]_____ and imprisonment for a period of _____.

(e) *Knowledge of or Intent to Cause Interference or Disruption of Critical Infrastructure*

Whoever commits interference and/or disruption pursuant to paragraphs (a) and (b) of this Section with the intent to cause or with knowledge that such conduct could cause interference and/or disruption of the computers, computer systems and/or connected systems, computer programs, computer data, content data, or traffic data used by critical infrastructure, shall have committed a criminal offense punishable by a fine of [amount]_____ and imprisonment for a period of _____.

(f) *Intent to Cause Interference or Disruption for Purposes of Terrorism*

Whoever commits interference and/or disruption pursuant to paragraphs (a) and (b) of this Section with the intent of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to acts of cyber terrorism, shall have committed a criminal offense punishable by a fine of

[amount]_____ and imprisonment for a period of _____.

Section 5
Interception

Whoever intentionally and without authorization pursuant to the rules of criminal procedure and any other laws of this country, intercepts, by technical means, non-public transmissions of computer data, content data, or traffic data, including electromagnetic emissions or signals from a computer, computer system, or network carrying or emitting such, to or from a computer, computer system and/or connected system, or network shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

Section 6
Misuse and Malware

(a) *Transmission of Malware and Misuse*

Whoever intentionally and without authorization causes the transmission of a computer program, information, code, or command with the intent of causing damage to a computer, computer system and/or connected system, network, computer program, content data, computer data, or traffic data shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(b) *Production, Sale, Procurement, Distribution of Computer or Computer Program for Access to Data and Misuse*

Whoever intentionally and without authorization engages in the production, sale, or procurement for use, import, distribution, or otherwise makes available:

(i) a computer or computer program, designed or adapted primarily for the purpose of committing any of the offenses established in Sections 2 through 5; and/or

(ii) a computer password, access code, or similar data by which the whole or part of any computer, computer system, network, computer program, computer data, content data, or traffic data may be accessed, with the intent that it be used for the purpose of committing any of the offenses established in

Sections 2 through 5; shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(c) *Possession of Computer or Computer Program for Access to Data or Misuse*

Whoever is in possession of one or more items referenced in (i) and (ii) of paragraph (b) of this Section with the intent that they be used for the purpose of committing any of the offenses established in Sections 2 through 5 shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(d) *No Penalty Without Intent to Commit Offense*

Notwithstanding the foregoing, this Section shall not be interpreted to impose criminal liability where the production, sale, procurement for use, import, distribution, or otherwise making available or possession of the items referenced in (i) and (ii) of paragraph (b) of this Section is not for the purpose of committing any of the offenses established in Sections 2 through 5, such as for the authorized testing or protection of computer systems and data.

(e) *Knowledge of or Intent to Cause Physical Injury*

Whoever commits an offense under paragraphs (a) or (b) of this Section with the intent to cause or with the knowledge that such conduct could cause physical injury to any person shall be punished by a fine of [amount]_____ and/or imprisonment for a period of _____.

(f) *Knowledge of or Intent to Cause Modification or Impairment of Medical Care*

Whoever commits an offense under paragraphs (a) or (b) of this Section with the intent to cause or with the knowledge that such conduct could cause the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals shall be punished by a fine of [amount]_____ and/or imprisonment for a period of _____.

(g) *Knowledge or Intent to Cause Threat to Public Safety or Public Health*

Whoever commits an offense under paragraph (a) of this Section with the intent to cause or with the knowledge that such conduct could cause a threat to public safety or public health shall be punished by a fine of [amount]_____ and/or imprisonment for a period of _____.

(h) *Intent to Furtherance of Terrorism*

Whoever commits an offense under paragraph (a) of this Section with the intent of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to cyber terrorism, shall be punished by a fine of [amount]_____ and imprisonment for a period of _____.

Section 7
Digital Forgery

Whoever intentionally and without authorization or legal right, engages in the input, acquisition, alteration, deletion, or suppression of a computer program, computer data, content data, or traffic data or otherwise alters the authenticity or integrity of such program or data, with the intent that it be considered or acted upon for legal purposes as though it were authentic or with integrity, regardless of whether or not the program or data is directly readable or intelligible, for any unlawful purpose, shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

Section 8
Digital Fraud, Procure Economic Benefit

(a) *Intent to Defraud*

Whoever knowingly and with intent to defraud, transfers, or otherwise disposes of, to another, or obtains control of with the intent to transfer or dispose of a computer password, access code, or similar data by which the whole or part of any computer program, computer, computer system, network, computer data, content data, or traffic data may be accessed shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(b) *Loss of Property to Procure Economic Benefit*

Whoever intentionally and without authorization or legal right causes the loss of property to another person through:

(i) the input, acquisition, alteration, deletion, or suppression of a computer program, computer data, content data, or traffic data; or

(ii) the interference with the functioning of a computer, computer system and/or connected system, or network; with the fraudulent or dishonest intent to procure an economic benefit for oneself or another shall have committed a criminal offense punishable by a fine of [amount] _____ and/or imprisonment for a period of _____.

Section 9
Extortion

(a) *Acts With Intent to Extort*

Whoever knowingly transmits any communication containing any threat to cause damage to a computer, computer system and/or connected system, network, computer program, computer data, content data, or traffic data with the intent to extort from any person any money or other thing of value shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(b) *Acts With Intent to Extort and Damage Government Computers, Data*

Whoever commits an offense under paragraph (a) of this Section and such action damages or could damage a

Government computer, computer system and/

or connected system, network, computer program, computer data, content data, or traffic data, shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(c) *Acts With Intent to Extort and Damage Critical Infrastructure Computers, Data*

Whoever commits an offense under paragraph (a) of this Section and such action damages or could damage a computer, computer system and/or connected system, network, computer program, computer data, content data, or traffic data of critical infrastructure shall have committed a criminal offense punishable by a fine of [amount]_____ and imprisonment for a period of _____.

Section 10
Aiding, Abetting, and Attempting

(a) Whoever intentionally aids or abets the commission of any of the offenses established in Sections 2 thorough 9 shall have committed a criminal offense punishable by a fine of [amount]_____ and imprisonment for a period of _____.

(b) Whoever intentionally attempts to commit any of the offenses established in Sections 2 thorough 9 shall have committed a criminal offense punishable by a fine of [amount]_____ and imprisonment for a period of _____.

Section 11
Corporate Liability

(a) *Acts Committed by Person in Senior or Leading Position*

Any legal person (corporation, association, or other legal entity) may be subject to civil, criminal, or administrative penalties for any offense established in Sections 2 through 10 if: (i) the offense was committed by a person holding a senior or leading position in the legal person; (ii) the senior or leading person acted (A) on his/her authority to represent the legal person, (B) on the authority vested in him/her to make decisions on behalf of the legal person, or (C) his/her authority to exercise control within the legal person; and (iii) the offense was committed for the benefit of the legal person.

(b) *Acts Committed by Employee or Agent Through Negligence of Senior or Leading Person*

Any legal person may be subject to civil, criminal, or administrative penalties for any offense established in Sections 2 through 10 if: (i) the offense was committed by an employee or agent of the legal person who was acting within the scope of his authority; (ii) the offense was committed for the benefit of the legal person; and (iii) the commission of the offense was made possible by the negligence of a senior or leading person that resulted in the failure to supervise the employee or agent through appropriate and reasonable measures intended to prevent employees or agents from committing criminal activities on behalf of the legal person. (c) Liability under paragraphs (a) and (b) of this Section shall be without prejudice to the criminal liability of the natural person who has committed the offense.

TITLE 3
PROCEDURAL PROVISIONS FOR CRIMINAL INVESTIGATIONS AND PROCEEDINGS FOR OFFENSES WITHIN THIS LAW

Section 12
Scope of Procedural Provisions

(a) The scope of the procedural provisions herein are for the purpose of specific criminal investigations or proceedings arising from offenses prohibited by Title 2 and the Substantive Provisions of this Law (Sections 2 through 10) and/or the laws of other jurisdictions that prohibit the same or similar actions. Except as provided otherwise in Section 5, pertaining to the interception of computer data, content data, or traffic data, these provisions apply to:

(i) the criminal offenses established in Section 2 through 10 of this Law;

(ii) other criminal offenses committed by means of a computer, computer system, or network; and

(iii) the collection of evidence in electronic form relating to such offenses.

Section 13
Conditions and Safeguards

(a) *Procedural Provisions*

The procedural provisions set forth in Title 3 of this Law are subject to the conditions and safeguards provided elsewhere in the Laws of this

country, including, but not limited to, judicial or other independent supervision, grounds justifying application, and limitation on the scope and duration of such power or procedure. These procedural provisions are also subject to the conditions and safeguards concerning human rights and liberties guaranteed under the laws of this country and international instruments, treaties, and laws, including the 1966 United Nations International Covenant on Civil and Political Rights.

(b) *Principle of Proportionality*

The procedural provisions set forth in Title 3 of this Law shall be conducted in compliance with the principal of proportionality, which shall be abided by in all criminal investigation activities performed by competent law enforcement bodies whenever evidence is to be gathered on and/or by means of electronic tools. Such criminal investigation activities include, but are not limited to, inspections, searches, seizure, custody, urgent inquiries, and searches for evidence. The impact of these procedural powers upon the rights, responsibilities, and legitimate interests of third parties alien to the facts investigated shall be considered when conducting such investigative activities.

Section 14
Preservation of Stored Computer Data, Content Data, Traffic Data

(a) The rules of criminal procedure for this country shall enable competent authorities to order or similarly obtain the expeditious preservation of specified computer data, content data, and/or traffic data that has been stored by means of a computer or computer system, particularly when there are grounds to believe that such data is particularly vulnerable to loss or modification.

(b) Where an order is issued to a person to preserve specified stored computer data, content data, or traffic data in a person's possession or control, that person shall preserve and maintain the integrity of such data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities of this country or of another jurisdiction to seek its disclosure. The integrity of such preserved data shall be documented by means of a mathematical algorithm and such record maintained along with the preserved data. Competent authorities may request that the preservation order be renewed.

(c) The custodian and any other person ordered to preserve such data shall keep confidential all information regarding such order for the period of time specified by the order or required under the Laws of this country.

(d) The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

Section 15
Expedited Preservation and Partial Disclosure of Traffic Data

(a) The rules of criminal procedure for this country shall provide: (i) for the expedited preservation of specified traffic data by a competent authority in this country, irrespective of whether one or more service providers are involved in the transmission of the subject communications; and (ii) the disclosure to competent authorities, or a designate of such authority, of a sufficient amount of traffic data to enable the identification of the service providers and the path through which the communication was transmitted.

(b) The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

Section 16
Expedited Preservation of Computers or Storage Media

(a) The rules of criminal procedure for this country shall enable competent authorities to order or similarly obtain the expeditious preservation of specified computers or storage media in situations in which there is an investigative, forensic, or practical necessity to do so to protect and preserve the computing environment to enable the extraction and examination of data and computing instructions, particularly when there are grounds to believe that such data is particularly vulnerable to loss or modification or when the preserving entity lacks the requisite capability to safely and effectively preserve the computing and/or content data external to the computer or storage media.

(b) Where an order is issued to a person to preserve specified computers and/or storage media in the person's possession or control, that person shall preserve and maintain the integrity of such computers and/or storage media for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities of this country or of another jurisdiction to

seek its disclosure. Competent authorities may request that the preservation order be renewed.

(c) The person and custodian ordered to preserve such computers and/or storage media shall keep confidential all information regarding such order for the period of time specified by the order.

(d) The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

Section 17
Production Order

Except as provided in Sections 19 and 20 of this Title, the rules of criminal procedure for this country shall enable a competent authority to order:

(a) a person to submit specified computer data, content data, and/or traffic data in that person's possession or control, which is stored in a computer, computer system, or a computer data storage medium; and

(b) a service provider providing services in this country to submit specified subscriber information relating to such services that is in that service provider's possession or control.

(c) The provisions of this Section are subject to the provisions of Sections 12 and 13.

Section 18
Search and Seizure of Stored Data

(a) *Search for Data*

The rules of criminal procedure for this country shall enable competent authorities, upon adequate reason and within the scope of legal approval, to search or similarly access: (i) a specified computer, computer system, computer program, or parts thereof, and/or the computer data, content data, and/or traffic data stored therein; and (ii) a computer data storage medium on which computer data, content data, or traffic data may be stored in this country.

(b) *Search in Connected Systems*

When the authorities seeking approval to conduct a search pursuant to paragraph (a) of this Section have grounds to believe that the data sought is stored in another computer system, or part of another system in this country, which is owned by or under the control of the same entity for which the scope of legal approval was granted, and such data is lawfully accessible from or available to the initial system, the rules of criminal procedure shall enable the authorities to expeditiously extend the search or similar accessing to the other system.

(c) *Seizure of Data*

The rules of criminal procedure for this country shall enable competent authorities to seize or similarly secure computer data, content data, or traffic data accessed pursuant to paragraphs (a) and (b) of this Section, including the power to: (i) seize or similarly secure a computer or computer system, or part of it, or a computer data storage medium; (ii) make and retain an image or copy of the computer data, content data, or traffic data; (iii) maintain the integrity of the relevant stored data and document such integrity by means of a mathematical algorithm which shall be maintained along with the stored computer data; and (iv) render inaccessible or remove those computer data in the accessed computer system.

(d) *Protection of Data*

The competent authorities in this country may order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs (a) and (b) of this Section.

(e) The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

Section 19
Interception (Real-Time Collection) of Traffic Data

(a) The competent authorities of this country may, upon adequate reason and within the scope of legal approval: (i) collect or record traffic data in real-time through technical means; (ii) compel a service provider, within its existing capability, to collect or record such traffic data in realtime or to cooperate and assist the competent authorities in the collection and recording of traffic data; associated with the specified communications in this country transmitted by means of a computer system and/or network.

(b) Any service provider requested to collect and record such traffic data in real-time or to cooperate or assist with such shall keep confidential the fact of the request and any information related to it.

(c) The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

Section 20
Interception (Real-Time Collection) of Content Data

(a) The competent authorities of this country may, upon adequate reason and within the scope of legal approval, collect or record through technical means, or compel a service provider, within its existing technical capability, to collect or record or to cooperate and assist the competent authorities in the collection and recording of content data, in real-time, of specified communications transmitted by means of a computer system.

(b) Any service provider requested to collect and record such content data in real-time or to cooperate or assist with such shall keep confidential the fact of the request and any information related to it.

(c) The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

TITLE 4
JURISDICTIONAL PROVISIONS

Section 21
Jurisdiction

(a) *Jurisdiction Over Persons and Domestic Acts*

This country shall have jurisdiction over any person, irrespective of his nationality or citizenship, who commits any offense established pursuant to Sections 2 through 10 of this Law when the offense is committed (i) within the territory of this country; (ii) using equipment, software, or data located within this country, regardless of the location of the perpetrator, or (iii) directed against equipment, software, or data located in this country, regardless of the location of the perpetrator.

(b) *Applicability to Acts on Ships and Aircrafts*

This country shall have jurisdiction over offenses committed pursuant to Sections 2 through 10 of this Law if the offense was committed (i) on board a ship flying the flag of this country; or (ii) on board an aircraft registered under the Laws of this country.

(c) *Applicability to Acts By Nationals Outside of Country*

This country shall have jurisdiction over offenses committed pursuant to Sections 2 through 10 of this Law if the offense was committed by a citizen or resident of this country and (i) if the offense is punishable under criminal law where it was committed; or (ii) if the offense is committed outside the territorial jurisdiction of any country.

(d) *Jurisdiction Where Extradition Refused*

In instances where an alleged offender is present in this country and this country elects to refuse a request for extradition of the alleged offender to another country on the basis of his or her nationality, jurisdiction over the stated offences shall be established in this country.

(e) *Concurrent Jurisdiction*

When another country claims jurisdiction over an offense within Sections 2 through 10 of this Law, the officials of the countries involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for the prosecution of the offense.

(f) *The Place Where the Offenses Occurred*

An offense is committed at every place the perpetrator acted (i) via his or her physical presence;[1] (ii) via the intentional use of equipment, software, or data,[2] or (iii) at any location which the resulting action is an element of an offense pursuant to Sections 2 through 10 of this Law occurred or would have occurred according to the understanding of the perpetrator.[3]

(g) *Reservation*

In specific cases, this country may reserve the right to apply or not to apply the jurisdictional rules in paragraphs (b) and (c) of this Section.

1 This includes, for example, the place where the perpetrator physically typed the command on a computer.
2 This would include, for example, the place where equipment or software intentionally used or attacked by the perpetrator is located, and thus would cover acts by foreign perpetrators located in another country but using attack servers or botnets located in another country.
3 This would include locations where the perpetrator thought the attack or action would impact. (i) international legal assistance in criminal matters; (ii) extradition; (iii) the identification, blocking, seizing or confiscation of the evidence, products, and instruments of the criminal offence; (iv) the carrying out of common investigations; (v) the exchange of information; (vi) technical assistance or assistance of any other nature for the collection of information; (vii) specialized personnel training; and (viii) other such activities deemed appropriate.

TITLE 5
INTERNATIONAL COOPERATION

Section 22
International Cooperation: General Principles

(a) The legal authorities of this country shall cooperate directly and to the widest extent possible with legal authorities of another country and/or with international organizations specializing in criminal matters for purposes of: (i) investigations or proceedings concerning criminal offenses related to computer programs, computers, computer systems, networks, computer data, content data, and/or traffic data; and/or (ii) the collection of evidence in electronic or any other form of a criminal offense. Such cooperation shall take place under the conditions of this Law and by observing: (i) the obligations that this country has assumed under international legal instruments on cooperation in criminal matters that this country is party to; (ii) arrangements agreed upon on the basis of uniform or reciprocal legislation in this regard; and (iii) the Laws of this country.

(b) The cooperation, organized and carried out according to paragraph (a) of this Section, may pertain to, as appropriate:

Section 23
Extradition Principles

(a) *Application of Extradition Provisions*

This Section applies to extradition between this country and another country, irrespective to whether there is an extradition treaty between this country and the requesting country, for the criminal offenses established pursuant to Sections 2 through 10 of this Law, provided that they are punishable under the laws of both countries and require deprivation of liberty for a maximum period of one year or longer.

(b) *Exception to Application of Extradition Principles*

Notwithstanding the foregoing, if the authorities of this country and another country agree on a different minimum penalty based upon uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between the countries, the minimum penalty provided for under such agreement or treaty shall apply.

(c) *Offenses in this Law are Extraditable*

The criminal offenses established pursuant to Sections 2 through 10 of this Law shall be deemed as extraditable offenses under any extradition treaty or agreement to which this country is a party and under all future treaties pertaining to extradition.

d. *Refusal of Extradition*

If extradition for a criminal offense pursuant to Sections 2 through 10 of this Law is refused solely on the basis of the nationality of the person sought or because this country desires to have jurisdiction over the offense, the competent legal authorities of this country shall submit the case to the appropriate authorities in this country for the purpose of prosecution and shall report the outcome to the requesting country in due course.

Section 24
Mutual Assistance: General Principles

(a) *Authority to Provide Mutual Assistance*

The competent authorities of this country shall provide assistance to another country to the widest extent possible for the purpose of investigations or proceedings concerning the criminal offenses established pursuant to Sections 2 through 10 of this Law and for the collection of evidence in electronic or other form. The rules of criminal procedure shall be amended to the extent necessary to support this requirement, including the procedures pertaining to mutual assistance requests in the absence of applicable international agreements.

(b) *Expedited Means of Communication*

Requests for and responses to requests for expedited mutual assistance may be made to the authorities of this country via the most efficient means, including facsimile or electronic mail, provided that appropriate levels of authentication and security are utilized and formal confirmation follows the request or response. The competent officials of this country shall respond to such requests by any such expedited means of communication.

(c) *Refusal to Cooperate*

Mutual assistance shall be provided in accordance with this Law or other Laws of this country or by mutual assistance treaties to which this country is obligated, including the grounds on which cooperation may be refused. Such assistance shall not be refused with respect to offenses pursuant to Sections 2 through 10 solely on the grounds that the request concerns a fiscal offense.

(d) *Dual Criminality*

Where mutual assistance from this country requires the existence of dual criminality, that condition shall be deemed fulfilled by this Law, irrespective of whether the offense in this country is in the same category of offenses or within the same terminology as the requesting country's law, provided that the offense is a criminal offense under the laws of the requesting country.

Section 25
Unsolicited Information

(a) The legal authorities of this country may forward to another country information obtained within its own investigations when it considers that the disclosure of such information may

(i) assist the other country in initiating or carrying out investigations or proceedings concerning criminal offenses similar to those established pursuant to Sections 2 through 10 of this Law, or

(ii) might lead to further cooperation with that country. Prior to providing such information, the legal authorities of this country may subject the data to confidentiality requirements or other conditions, but shall not forward such information unless such requirements or conditions are accepted by the other country.

Section 26
Procedures for Mutual Assistance

(a) *Application of this Section and Central Authority*

The rules of criminal procedure for this country shall specify a central authority responsible for sending and answering requests for mutual assistance. Such central authority shall answer requests for mutual assistance, execute such requests, and or transmit requests to the appropriate authorities competent for their execution.

Such central authority shall communicate with similar authorities in requesting countries.

If there is a mutual assistance treaty or reciprocal or uniform law between the requesting country and this country, the provisions of this Section may apply upon mutual agreement of this country and the requesting country. If there is no such mutual assistance treaty or reciprocal or uniform law, the provisions of this Section shall apply.

(b) *Rules of Procedure for Mutual Assistance*

Mutual assistance requests shall be handled according to the procedures of the requesting country unless they are incompatible with the rules of criminal procedure of this country, in which case the rules of this country shall take precedence.

(c) *Refusal to Assist*

The central authority responsible for sending and answering requests for mutual assistance may refuse to provide mutual assistance if: (i) such request is against the laws of this country, except refusal shall not be allowed for offenses within Sections 2 through 10 of the Law on the grounds that they are considered a fiscal offense; (ii) such request concerns an offense which the competent authorities of this country consider a political offense or an offense connected to a political offense; or (iii) execution of the request is likely to prejudice the sovereignty of this country, its security, public order and safety, or other essential interests. The central authority may postpone action on a mutual assistance request if such action would prejudice criminal or investigations or proceedings within this country, however, the central authority shall first consider whether the request may be partially granted or subjected to conditions.

(d) *Inform of Outcome of Assistance*

The rules of criminal procedure shall establish a process for the central authority to promptly inform the requesting country of the outcome of any requests for assistance, with reasons provided for postponement, refusal, or circumstances which would delay the assistance or render it impossible.

(e) *Confidentiality of Request*

The central authority shall (i) keep confidential the fact of the request and its subject, if so requested by the requesting country, except to the extent necessary to execute the request, or (ii) provide an explanation to the requesting country why such confidentiality is not possible to enable the requesting country to determine if the request should be nevertheless executed.

(f) *Urgent Requests or Requests Not Involving Coercive Action*

Urgent requests for mutual assistance or requests not involving coercive action may be

sent: (i) directly by judicial authorities of the requesting country to the competent judicial authority of this country, with a copy of such request sent to the central authorities of both countries, understanding that the judicial authority of this country may, in its discretion, refer the matter to the central authority; or (ii) to the International Criminal Police Organization (Interpol), with a copy of such request sent to the central authority.

(g) *Confidentiality of Information to be Provided*

This country may supply the requested information upon the condition that it be kept confidential or that it shall not be used for investigations or proceedings other than those stated in the request. If the requesting country cannot comply with such conditions, the legal authorities in this country shall determine whether the requested information shall nevertheless be provided and the central authority shall communicate such decision to the requesting country. The competent authorities in this country supplying any such information shall require the receiving party to abide by any confidentiality requirements and to provide an explanation regarding the use made of the information provided.

Section 27
Expedited Preservation of Stored Computer Data, Content Data, or Traffic Data

(a) *Request for Expedited Preservation*

Within mutual assistance, the competent authorities of a country may request the expeditious preservation of specified computer data, content data, or traffic data located within the territory of this country, in respect of which the requesting country intends to submit a request for mutual assistance for the search or for access, seizure, or similar securing or disclosure of the data.

(b) *Content of Request for Expedited Preservation*

The request for expedited preservation referred to in paragraph (a) of this Section shall specify:

(i) the authority requesting the preservation;

(ii) the offense that is the subject of a criminal investigation or proceeding and a brief statement of the related facts;

(iii) the stored computer data, content data, and/or traffic data to be preserved and its relationship to the offense;

(iv) any available information identifying the custodian of such stored data or the location of the computer or computer system(s) containing the data;

(v) the necessity of the preservation; and

(vi) that the requesting country intends to submit a request for mutual assistance for the search or for access, seizure, or similar securing or disclosure of the subject data.

(c) *Measures to be Taken*

Upon receipt of such a request, the competent authorities of this country shall take all appropriate measures to preserve expeditiously the specified data in accordance with the Laws of this country. Dual criminality shall [or shall not] be required for such preservation.

(d) *Refusal of Preservation*

A request for preservation may only be refused if the request concerns an offense that this country considers a political offense or an offense connected with such, or this country determines that the execution of the request is likely to prejudice its sovereignty, security, public safety, or other essential interests.

(e) *Where Preservation May Not Ensure Availability*

Where the competent legal authorities believe that the requested preservation will not ensure the future availability of the data or will threaten the confidentiality or otherwise prejudice the other country's investigation, the legal authorities shall promptly inform the requesting country, which may then determine if the preservation should nevertheless be executed.

(f) *Duration of Preservation*

No preservation effected under this Section shall be for a period of less than sixty (60) days to enable the requesting country to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such request, the data shall continue to be preserved pending a decision on the request.

Section 28
Expedited Disclosure of Preserved Content Data, Computer Data, or Traffic Data

(a) If, in executing a request for preservation according to Section 27 of this Law, the legal authorities of this country discover that a service provider in another country was involved in the transmission of the communication, the legal authorities shall promptly disclose to the requesting country a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

(b) Disclosure of traffic data, as prescribed by paragraph (a) of this Section, may only be withheld from the requesting country if:

(i) the request concerns an offense that this country considers a political offense or an offense connected with such an offense; or

(ii) the legal authorities of this country consider that the execution of the request is likely to prejudice its sovereignty, security, public safety, or other essential interests.

Section 29
Mutual Assistance Regarding Access to Stored Computer Data, Content Data, or Traffic Data

(a) The competent officials of another country may request the competent officials of this country to search or similarly access, seize or similarly secure, and disclose specified data stored by means of a computer or computer system located within the territory of this country, including data that has been preserved pursuant to Section 27 of this Law. Such requests shall adhere to the principles pertaining to international cooperation in Section 22 of this Law and shall comply with other relevant provisions of this Law.

(b) Requests pursuant to paragraph (a) of this Section shall be responded to on an expedited basis where

(i) there are grounds to believe that the requested data is particularly vulnerable to loss or modification; or

(ii) expedited cooperation is provided according the instruments, arrangements, and laws referred to in Section 22 of this Law.

Section 30
Trans-Border Access to Stored Computer Data, Content Data, or Traffic Data

(a) A competent authority may access publicly available (open source) stored computer data, content data, or traffic data regardless of where the data is located geographically.

(b) A competent authority from another country may, without authorization of authorities of this country, have access to and receive, by means of a computer or computer system located on its territory, specified computer data, content data, or traffic data stored in this country if the competent authority from the other country obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to such competent authority through that computer or computer system.

Section 31
Mutual Assistance In Real-Time Collection of Traffic Data

(a) The competent authorities of this country shall provide mutual assistance to the competent authorities of another country with respect to the real-time collection of specified traffic data associated with specified communications in the territory of this country that were transmitted by means of a computer or computer system. Subject to the provisions of paragraph (b) of this Section, this assistance shall be governed by the Laws and rules of criminal procedure for this country.

(b) The competent authorities of this country shall provide assistance pursuant to paragraph (a) of this Section for criminal cases in a manner equal to that which would be available in a similar domestic case.

Section 32
Mutual Assistance Regarding Interception of Content Data or Computer Data

The competent authorities of this country shall provide mutual assistance to the competent authorities of another country in the real-time collection or recording of specified computer data or content data of specified communications transmitted by means of a computer or computer system to the extent permitted under the Laws of this country and treaties to which this country is bound.

Section 33
24/7 Points of Contact

(a) The competent authorities of this country shall designate points of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offenses related to computers, computer systems, networks, computer data, content data, and/or traffic data, or for the collection of other evidence in electronic form related to a criminal offense. Such assistance shall include facilitating, or if permitted under the Laws of this country and the practices of competent authorities, directly carrying out the following measures: (i) the provision of technical advice; (ii) the preservation of data pursuant to Sections 27 and 28; and (iii) the collection of evidence, the provision of legal information, and locating of suspects.

(b) The points of contact shall have the capacity to carry out communications with the points of contact in other countries on an expedited basis. If the designated points of contact are not responsible for international cooperation and mutual assistance or extradition, the points of contact shall ensure that they are able to coordinate with such authorities on an expedited basis.

(c) The competent authorities of this country shall ensure that all points of contact are properly trained and equipped or that other trained personnel are available to the points of contact to facilitate the operation of the network and compliance with the provisions of this Law.

TITLE 6
PROVISIONS APPLICABLE TO OTHER OFFENSES

Section 34
Provisions That Apply to Other Offenses

The competent authorities of this country may, upon adequate reason and within the scope of legal approval and the Laws of this country and/or any legal obligations that this country may be subject to through

(a) the Bern Convention for the Protection of Literary and Artistic Works,

(b) the Agreement on Trade-Related Aspects of Intellectual Property Rights,

(c) the WIPO Copyright Treaty,

(d) the International Convention for the Protection of Performers, Producers, Phonograms, and Broadcasting Organization,

(e) the WIPO Performance and Phonograms Treaty, and/or

(f) any international agreements or treaties pertaining to child pornography may exercise the authority granted in Sections 12-32 of this Law to investigate or assist in the investigation of offenses related to such Laws or legal obligations. The provisions of this Section are subject to the Provisions of Sections 12 and 13 of this Law.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)

THE COUNCIL,

Having regard to articles 1(c), 3(a) and 5(b) of the Convention on the Organisation for Economic Co-operation and Development of 14th December, 1960;

RECOGNISING:

that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;

that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;

that transborder flows of personal data contribute to economic and social development; that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

RECOMMENDS:

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;
2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;
3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;
4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

Annex to the Recommendation of the Council of 23rd September 1980 Guidelines governing the protection of privacy and transborder flows of personal data

PART ONE
GENERAL DEFINITIONS

1. For the purposes of these Guidelines:
   a. "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;
   b. "personal data" means any information relating to an identified or identifiable individual (data subject);
   c. "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.
3. These Guidelines should not be interpreted as preventing:
   a. the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;
   b. the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or
   c. the application of the Guidelines only to automatic processing of personal data.
4. Exceptions to the Principles contained in Parts

Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

a. as few as possible, and

b. made known to the public.

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO
BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

    a. with the consent of the data subject; or

    b. by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

    a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

    b. to have communicated to him, data relating to him

        - within a reasonable time;
        - at a charge, if any, that is not excessive;
        - in a reasonable manner; and
        - in a form that is readily intelligible to him;

    c. to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

    d. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE
BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR
NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

    a. adopt appropriate domestic legislation;

    b. encourage and support self-regulation, whether in the form of codes of conduct or otherwise;

    c. provide for reasonable means for individuals to exercise their rights;

    d. provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and

    e. ensure that there is no unfair discrimination against data subjects.

PART FIVE
INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate information exchange related to these Guidelines, and mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

Guidelines for the Security of Information Systems and Networks (2002)

THE COUNCIL,

Having regard to the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960, in particular, Articles 1 b), 1 c), 3 a) and 5 b) thereof; *Having regard* to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)];

Having regard to the Declaration on Transborder Data Flows adopted by the Governments of OECD Member countries on 11 April 1985 [Annex to C(85)139];

Having regard to the Recommendation of the Council concerning Guidelines for Cryptography Policy of 27 March 1997 [C(97)62/FINAL];

Having regard to the Ministerial Declaration on the Protection of Privacy on Global Networks of 7-9 December 1998 [Annex to C(98)177/FINAL];

Having regard to the Ministerial Declaration on Authentication for Electronic Commerce of 7-9 December 1998 [Annex to C(98)177/FINAL];

Recognising that information systems and networks are of increasing use and value to governments, businesses, other organisations and individual users;

Recognising that the increasingly significant role of information systems and networks, and the growing dependence on them for stable and efficient national economies and international trade and in social, cultural and political life call for special efforts to protect and foster confidence in them;

Recognising that information systems and networks and their worldwide proliferation have been accompanied by new and increasing risks;

Recognising that data and information stored on and transmitted over information systems and networks are subject to threats from various means of unauthorised access, use, misappropriation, alteration, malicious code transmissions, denial of service or destruction and require appropriate safeguards;

Recognising that there is a need to raise awareness of risks to information systems and networks and of the policies, practices, measures and procedures available to respond to those risks, and to encourage appropriate behaviour as a crucial step towards the development of a culture of security;

Recognising that there is a need to review current policies, practices, measures, and procedures to help assure that they meet the evolving challenges posed by threats to information systems and networks;

Recognising that there is a common interest in promoting the security of information systems and networks by means of a culture of security that fosters international co-ordination and co-operation to meet the challenges posed by the potential harm from security failures to national economies, international trade and participation in social, cultural and political life;

And further recognising that the Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security set out in the Annex to this Recommendation are voluntary and do not affect the sovereign rights of nations;

And recognising that these Guidelines are not meant to suggest that any one solution exists for security or what policies, practices, measures and procedures are appropriate to any particular situation, but rather to provide a framework of principles to promote better understanding of how participants may both benefit from, and contribute to, the development of a culture of security;

COMMENDS these Guidelines for the Security of the Information Systems and Networks: Towards a Culture of Security to governments, businesses, other organisations and individual users who develop, own, provide, manage, service, and use information systems and networks;

RECOMMENDS that Member countries:

Establish new, or amend existing, policies, practices, measures and procedures to reflect and take into account the Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security by adopting and promoting a culture of security as set out in the Guidelines;

Consult, co-ordinate and co-operate at national and international levels to implement the Guidelines;

Disseminate the Guidelines throughout the public and private sectors, including to governments, business, other organisations, and individual users to promote a culture of security, and to encourage all concerned parties to be responsible and to take necessary steps to implement the Guidelines in a manner appropriate to their individual roles;

Make the Guidelines available to non-member countries in a timely and appropriate manner;

Review the Guidelines every five years so as to foster international co-operation on issues relating to the security of information systems and networks;

INSTRUCTS the OECD Committee for Information, Computer and Communication Policy to promote the implementation of the Guidelines.

This Recommendation replaces the Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26 November 1992

[C(92)188/FINAL].

Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam (2006)

THE COUNCIL,

Having regard to the Convention on the Organisation for Economic Co-operation and Development of 14th December 1960, in particular Article 5 (b) thereof;

Recognising that spam undermines consumer confidence, which is a prerequisite for the information society and for the success of e-commerce;

Recognising that spam can facilitate the spread of viruses, serve as the vehicle for traditional fraud and deception as well as for other Internet-related threats such as phishing, and that its effects can negatively impact the growth of the digital economy, thus resulting in important economic and social costs for Member countries and non-member economies;

Recognising that spam poses unique challenges for law enforcement in that senders can easily hide their identity, forge the electronic path of their email messages, and send their messages from anywhere in the world to anyone in the world, thus making spam a uniquely international problem that can only be efficiently addressed through international co-operation;

Recognising the need for global co-operation to overcome a number of challenges to information gathering and sharing, for identifying enforcement priorities and for developing effective international enforcement frameworks;

Recognising that current measures, such as numerous bi- and multilateral criminal law enforcement co-operation instruments, provide a framework for enforcement co-operation on criminal conduct associated with spam, such as malware and phishing;

Having regard to the Recommendation of the Council concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (hereinafter "Cross-border Fraud Guidelines"), which sets forth principles for international co-operation among consumer protection enforcement agencies in combating cross-border fraud and deception [C(2003)116];

Having regard to the Recommendation of the Coun-

cil concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58] (hereinafter "Privacy Guidelines"), and the Ministerial Declaration on the Protection of Privacy on Global Networks [C(98)177];

Recognising that, in some instances, the Cross-border Fraud Guidelines and the Privacy Guidelines may apply directly to cross-border spam enforcement co-operation and that even where this is not the case, many of the principles expressed in these Guidelines can be usefully tailored to develop appropriate national frameworks and facilitate international co-operation to enforce laws against spam;

Recalling that, while cross-border enforcement co-operation is an important element in tackling the global problem of spam, it is necessary in this respect to adopt a comprehensive national approach which also addresses regulatory and policy issues, facilitates the development of appropriate technical solutions, improves education and awareness among all players and encourages industry-driven initiatives;

On the joint proposal of the Committee for Information, Computer and Communications Policy and the Committee on Consumer Policy:

AGREES that:

For the purposes of this Recommendation, and without prejudice to other existing co-operation instruments "Spam Enforcement Authorities" means any national public body, as determined by each Member country, that is responsible for enforcing Laws Connected with Spam and has powers to (a) co-ordinate or conduct investigations or (b) pursue enforcement proceedings, or (c) both.

For the purposes of this Recommendation, "Laws Connected with Spam" means (a) laws specifically targeting electronic communications; or (b) general laws, such as privacy laws, consumer protection laws or telecommunication laws that may apply to electronic communications.

This Recommendation is primarily aimed at national public bodies, with enforcement authority for Laws Connected with Spam. It is recognised that some Member countries have many competent bodies, some of which are regional or local, that can take or initiate action against spam. It is also recognised that, in some Member countries, private enforcement bodies may play a very important role in ensuring enforcement of Laws Connected with Spam, including in cross-border situations.

This Recommendation covers cross-border spam enforcement co-operation only in areas where the conduct prohibited by the Laws Connected with Spam of the Member country receiving a request for assistance is substantially similar to conduct prohibited by the Laws Connected with Spam of the Member country requesting assistance. Co-operation under this Recommendation does not affect the freedom of expression as protected in laws of Member countries.

Co-operation under this Recommendation focuses on those violations of Laws Connected with Spam that are most serious in nature, such as those that (a) cause or may cause injury (financial or otherwise) to a significant number of recipients, (b) affect particularly large numbers of recipients (c) cause substantial harm to recipients.

In all instances, the decision on whether to provide assistance under this Recommendation rests with the Spam Enforcement Authority receiving the request for assistance.

This Recommendation encourages Member countries to cooperate in this area under any other instruments, agreements, or arrangements.

RECOMMENDS that:

Member countries work to develop frameworks for closer, faster, and more efficient co-operation among their Spam Enforcement Authorities that includes, where appropriate:

a. *Establishing a domestic framework.*

Member countries should in this respect:

(i) Introduce and maintain an effective framework of laws, Spam Enforcement Authorities, and practices for the enforcement of Laws Connected with Spam.

(ii) Take steps to ensure that Spam Enforcement Authorities have the necessary authority to obtain evidence sufficient to investigate and take action in a timely manner against violations of Laws Connected with Spam that are committed from their territory or cause effects in their territory. Such authority should include the ability to obtain necessary information and relevant documents.

(iii) Improve the ability of Spam Enforcement Authorities to take appropriate action against (a) senders of electronic communications that violate Laws Connected with Spam and (b) individuals or companies that profit from the sending of such communications.

(iv) Review periodically their own domestic frameworks and take steps to ensure their effectiveness for cross-border co-operation in the enforcement of Laws Connected with Spam.

(v) Consider ways to improve redress for financial injury caused by spam.

b. *Improving the ability to cooperate.*

Member countries should improve the ability of their Spam Enforcement Authorities to cooperate with foreign Spam Enforcement Authorities.

Member countries should in this respect:

(i) Provide their Spam Enforcement Authorities with mechanisms to share relevant information with foreign authorities relating to violations of their Laws Connected with Spam upon request, in appropriate cases and subject to appropriate safeguards.

(ii) Enable their Spam Enforcement Authorities to provide investigative assistance to foreign authorities relating to violations of their Laws Connected with Spam upon request, in appropriate cases and subject to appropriate safeguards, in particular with regard to obtaining information from persons; obtaining documents or records; or locating or identifying persons or things.

(iii) Designate a contact point for co-operation under this Recommendation and provide the OECD Secretariat with updated information regarding their Laws Connected with Spam and the Spam Enforcement Authority designated as the contact point. The OECD Secretariat will keep record of this information and make it available to interested parties.

c. *Improving procedures for co-operation.*

Before making requests for assistance as foreseen in the previous paragraphs, Spam Enforcement Authorities should:

(i) Proceed to some preliminary investigative work to determine whether a request for assistance is warranted, and is consistent with the scope and priorities set forth by this Recommendation.

(ii) Attempt to prioritise requests for assistance and, to the extent possible, make use of common resources such as the OECD Website on spam, informal channels, existing international networks and existing law enforcement co-operation instruments to implement this Recommendation.

d. *Cooperating with relevant private sector entities.*

Spam Enforcement Authorities, businesses, industry groups, and consumer groups should cooperate in pursuing violations of Laws Connected with Spam. In particular, Spam Enforcement Authorities should cooperate with these groups on user education, promote their referral of relevant complaint data, and encourage them to share with Spam Enforcement Authorities investigation tools and techniques, analysis, data and trend information.

Member countries should encourage co-operation between Spam Enforcement Authorities and the private sector to facilitate the location and identification of spammers.

Member countries should also encourage participation by private sector and non-member economies in international enforcement co-operation efforts; efforts to reduce the incidence of inaccurate information about holders of domain names; and efforts to make the Internet more secure.

Where appropriate, Spam Enforcement Authorities and the private sector should continue to explore new ways to reduce spam.

INVITES non-member economies to take due account of this Recommendation and collaborate with Member countries in its implementation.

INSTRUCTS the Committee for Information, Computer and Communications Policy and the Committee on Consumer Policy to monitor the progress in cross-border enforcement co-operation in the context of this Recommendation within three years of its adoption and thereafter as appropriate.

BIAC and MAAWG Best Practices for Internet Service Providers and Network Operators[1]

Background

ISPs and network operators have an important role in the fight against spam.

Given this important role, ISPs, network operators, technical groups and alliances continue to share best practices for preventing/diminishing spam sent from or across their networks.

Although best practices will not, in and of themselves, constitute a comprehensive solution to spam, they are part of a multi-prong strategy for addressing the problem of spam. The larger the number of entities endorsing and applying common practices, the more effective they will be.

In the vent that these voluntary Best Practices are taken up by ISPs and Network Operators, their positive impact will be increased if end-users also take necessary steps to protect the security of their computers, software and networks, including the protection of their personal identity on-line.

Intent

BIAC's Best Practices for ISPs and Network Operators are a set of voluntary principles developed by business aimed at enhancing the security of network infrastructures in the fight against Spam. Industry will continue to collaborate on additional technical and procedural measures to further implement these principles.

BIAC proposes the following Best Practices for ISPs and Network Operators as an important tool in combating Spam. These Best Practices and any additional measures are voluntary, and in all cases precedence is given to applicable legal and regulatory frameworks.

Implementation of these Best Practices and any additional measures will vary, depending on the technical configurations of particular providers'/operators' networks, and their specific business needs and challenges. We note that flexibility in the implementation of these Best Practices and any additional measures is the key to achieving their broad and meaningful adoption by service providers of all sizes.

Given the rapid pace of technological change, the Best Practices will be periodically reviewed and updated.2

Best Practices

Context/Definitions

In any given national jurisdiction, each of the Best Practices is understood to be recommended only if it is not in contradiction with existing national legislation.

In the context of these Best Practices "ISPs and network operators" include any entity operating a SMTP server connected to the Internet.

BIAC Recommends to ISPs and Network Operators that:

1. Within the boundaries of the appropriate legal framework, ISPs and network operators address the problem of compromised end-user equipment by establishing timely processes to allow such end-user equipment and network elements to be managed and eliminated as sources of Spam;
2. ISPs and network operators utilize industry standard technology to authenticate their email and/or their sources;
3. ISPs and network operators block potentially infecting email file attachments. In the case of filtering email or email file attachments based on content properties, in the context of any required legislation prior agreement is to be attained from the customer;
4. ISPs and network operators actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and the source of such activity, and respond appropriately;

1 BIAC was created in March 1962 as an independent organisation recognised by the OECD as the official representative of the OECD business community (http://www.biac.org). BIAC's members are the major industrial and employers' organisations in the 30 OECD member countries, representing over 8 million companies. Via its 31 standing committees and policy groups, BIAC mirrors all economic policy issues the OECD covers and examines their potential impacts on business in both member and an increasing number of non-member countries like Russia, China and India.
The Messaging Anti-Abuse Working Group (http://www.MAAWG.org) is a global organization focusing on preserving electronic messaging from online exploits and abuse with the goal of enhancing user trust and confidence, while ensuring the deliverability of legitimate messages. With a broad base of Internet Service Providers (ISPs) and network operators representing over 600 million mailboxes, key technology providers and senders, MAAWG works to address messaging abuse by focusing on technology, industry collaboration and public policy initiatives.

5. ISPs and network operators establish appropriate inter-company processes for reacting to other network operators' incident reports, also accepting end user complaints.

6. ISPs, network operators and enterprise email providers communicate their security policies and procedures to their subscribers;

7. ISPs and network operators attempt to send non-delivery notices (NDNs) only for messages originated by their own account holders;

8. ISPs and network operators take measures to ensure that only their account holders use their e-mail submit servers;

9. ISPs and network operators ensure that all domain names, Domain Name System (DNS) records and applicable Internet protocol (IP) address registration records (e.g. WHOIS, Shared WHOIS Project [SWIP] or referral WHOIS [RWHOIS]) are responsibly maintained with correct, complete and current information, and that this information includes points of contact for roles responsible for resolving abuse issues including, but not limited to, postal address, phone number and email address;

10. ISPs and network operators ensure that all their publicly routable and Internet-visible IP addresses have appropriate and up-to-date forward and reverse DNS records and WHOIS and SWIP entries; that all local area network (LAN) operators are compliant with Request for Comments (RFCs) 1918 — "Address Allocation for Private Internets," and that in particular, LANs do not use IP space globally registered to someone else, or IP space not registered to anyone, as private IP space.

Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (2003)

THE COUNCIL,

Having regard to the Convention on the Organisation for Economic Co-operation and Development of 14th December 1960, in particular, Article 5 b) thereof;

Having regard to the Ministerial Declaration on Consumer Protection in the Context of Electronic Commerce of 8 October 1998 [C(98)177(Annex 2)];

Having regard to the Recommendation of the Council concerning Guidelines for Consumer Protection in the Context of Electronic Commerce, adopted on 9 December 1999 [C(99)184/FINAL], which states that Member countries should, through "their judicial, regulatory, and law enforcement authorities co-operate at the international level, as appropriate, through information exchange, co-ordination, communication and joint action to combat cross-border fraudulent, misleading and unfair commercial conduct," and which further states that "governments, businesses, consumers and their representatives should devote special attention to the development of effective cross-border redress systems";

Recognising that fraudulent and deceptive commercial practices against consumers undermine the integrity of both domestic and global markets to the detriment of all businesses and consumers, and undermine consumer confidence in those markets;

Recognising that most existing laws and enforcement systems designed to address fraudulent and deceptive commercial practices against consumers were developed at a time when such practices were predominantly domestic, and that such laws and systems are therefore not always adequate to address the emerging problem of cross-border fraudulent and deceptive commercial practices;

Recognising that, despite differing national systems and laws for the protection of consumers, a consensus exists on the need for a common framework to enable the further development of close co-operation among consumer protection enforcement agencies, to tackle cross-border fraudulent and deceptive commercial practices;

Recognising that closer co-operation in combating fraudulent and deceptive commercial practices can

lay the groundwork for enhanced international co-operation on a larger number of consumer protection issues in the future;

RECOMMENDS:

That consumer protection enforcement agencies in Member countries, having a common interest in preventing fraudulent and deceptive commercial practices against consumers, co-operate with one another in enforcing their laws against such practices;

That Member countries work to develop a framework for closer, faster, and more efficient co-operation amongst their consumer protection enforcement agencies that includes where appropriate:

- Establishing a domestic system for combating cross-border fraudulent and deceptive commercial practices against consumers.
- Enhancing notification, information sharing, and investigative assistance.
- Improving the ability to protect foreign consumers from domestic businesses engaged in fraudulent and deceptive commercial practices.
- Improving the ability to protect domestic consumers from foreign businesses engaged in fraudulent and deceptive commercial practices.
- Considering how to ensure effective redress for victimised consumers. And
- Co-operating with relevant private sector entities.

That Member countries implement this Recommendation, as set forth in greater detail in the Guidelines contained in the Annex thereto and of which it forms an integral part;

That non member economies be invited to take account of this Recommendation, with appropriate implementation assistance from Member countries;

DECIDES that the Secretary-General shall keep a record of the consumer protection enforcement or policy agency designated as a contact point, and advise Member countries of modifications to this record; and

INSTRUCTS the Committee on Consumer Policy to exchange information on progress and experiences regarding the implementation of this Recommendation, review that information, and report to the Council on this subject within three years of the adoption of this Recommendation and thereafter as appropriate.

Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007)[2]

THE COUNCIL,

Having regard to articles 1, 3, and 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14th December 1960;

Having regard to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL], which recognizes that Member countries have a common interest in protecting individuals' privacy without unduly impeding transborder data flows, and states that Member countries should establish procedures to facilitate "mutual assistance in the procedural and investigative matters involved";

Having regard to the Declaration on the Protection of Privacy on Global Networks [C(98)177, Annex 1], which recognizes that different effective approaches to privacy protection can work together to achieve effective privacy protection on global networks and states that Member countries will take steps to "ensure that effective enforcement mechanisms" are available both to address non-compliance with privacy principles and to ensure access to redress;

Having regard to the Recommendation of the Council concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders [C(2003)116)] and the Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws against Spam [C(2006)57], which set forth principles for international law enforcement co-operation in combating cross-border fraud and deception and illegal spam, respectively, and which illustrate how cross-border co-operation among Member countries can be improved;

Recognizing the benefits in terms of business efficiency and user convenience that the increase in transborder flows of data has brought to organizations and individuals;

Recognizing that the increase in these flows, which include personal data, has also raised new challenges and concerns with respect to the protection of privacy;

Recognizing that, while there are differences in their laws and enforcement mechanisms, Member countries share an interest in fostering closer international co-operation among their privacy law enforcement authorities as a means of better safeguarding personal data and minimizing disruptions to transborder data flows;

Recognizing that, although there are regional instruments and other arrangements under which such co-operation will continue to take place, a more global and comprehensive approach to this co-operation is desirable;

On the proposal of the Committee for Information, Computer and Communications Policy:

RECOMMENDS:

That Member countries co-operate across borders in the enforcement of laws protecting privacy, taking appropriate steps to:

e. Improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities.

f. Develop effective international mechanisms to facilitate cross-border privacy law enforcement co-operation.

g. Provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing, subject to appropriate safeguards.

h. Engage relevant stakeholders in discussion and activities aimed at furthering co-operation in the enforcement of laws protecting privacy.

That Member countries implement this Recommendation, as set forth in greater detail in the Annex, of which it forms an integral part.

INVITES non-Member economies to take account of the Recommendation and collaborate with Member countries in its implementation.

INSTRUCTS the Committee for Information, Computer and Communications Policy to exchange information on progress and experiences with respect

2 This Recommendation was developed by the OECD Committee for Information, Computer and Communications Policy (ICCP), through its Working Party on Information Security and Privacy (WPISP). The work was led by Jennifer Stoddart, Privacy Commissioner of Canada, with the support of a number of representatives from privacy enforcement authorities participating as part of their country delegations. It has also benefited from a constructive consultation with other key stakeholders in the privacy and data protection community. It was adopted as a Recommendation of the OECD Council on 12 June 2007.

to the implementation of this Recommendation, review that information, and report to the Council within three years of its adoption and thereafter as appropriate.

ANNEX

I. DEFINITIONS

1. For the purposes of this Recommendation:

   a. "Laws Protecting Privacy" means national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with the OECD Privacy Guidelines.

   b. "Privacy Enforcement Authority" means any public body, as determined by each Member country, that is responsible for enforcing Laws Protecting Privacy, and that has powers to conduct investigations or pursue enforcement proceedings.

II. OBJECTIVES AND SCOPE

2. This Recommendation is intended to foster international co-operation among Privacy Enforcement Authorities to address the challenges of protecting the personal information of individuals wherever the information or individuals may be located. It reflects a commitment by Member countries to improve their enforcement systems and laws where needed to increase their effectiveness in protecting privacy.

3. The main focus of this Recommendation is the authority and enforcement activity of Privacy Enforcement Authorities. However, it is recognised that other entities, such as criminal law enforcement authorities, privacy officers in public and private organisations and private sector oversight groups, also play an important role in the effective protection of privacy across borders, and appropriate co-operation with these entities is encouraged.

4. Given that cross-border co-operation can be complex and resource-intensive, this Recommendation is focused on co-operation with respect to those violations of Laws Protecting Privacy that are most serious in nature. Important factors to consider include the nature of the violation, the magnitude of the harms or risks as well as the number of individuals affected.

5. Although this Recommendation is primarily aimed at facilitating co-operation in the enforcement of Laws Protecting Privacy governing the private sector, Member countries may also wish to co-operate on matters involving the processing of personal data in the public sector.

6. This Recommendation is not intended to interfere with governmental activities relating to national sovereignty, national security, and public policy ("ordre public").

III. DOMESTIC MEASURES TO ENABLE CO-OPERATION

7. In order to improve cross-border co-operation in the enforcement of Laws Protecting Privacy, Member countries should work to develop and maintain effective domestic measures that enable Privacy Enforcement Authorities to co-operate effectively both with foreign and other domestic Privacy Enforcement Authorities.

8. Member countries should review as needed, and where appropriate adjust, their domestic frameworks to ensure their effectiveness for cross-border co-operation in the enforcement of Laws Protecting Privacy.

9. Member countries should consider ways to improve remedies, including redress where appropriate, available to individuals who suffer harm from actions that violate Laws Protecting Privacy wherever they may be located.

10. Member countries should consider how, in cases of mutual concern, their own Privacy Enforcement Authorities might use evidence, judgments, and enforceable orders obtained by a Privacy Enforcement Authority in another country to improve their ability to address the same or related conduct in their own countries.

A. *Providing effective powers and authority*

11. Member countries should take steps to ensure that Privacy Enforcement Authorities have the necessary authority to prevent and act in a timely manner against violations of Laws Protecting Privacy that are committed from their territory or cause effects in their territory. In particular, such authority should include effective measures to:

    a. Deter and sanction violations of Laws Protecting Privacy;

    b. Permit effective investigations, including the ability to obtain access to relevant information, relating to possible violations of Laws Protecting Privacy;

c. Permit corrective action to be taken against data controllers engaged in violations of Laws Protecting Privacy.

B. *Improving the ability to co-operate*

12. Member countries should take steps to improve the ability of their Privacy Enforcement Authorities to co-operate, upon request and subject to appropriate safeguards, with foreign Privacy Enforcement Authorities, including by:

    a. Providing their Privacy Enforcement Authorities with mechanisms to share relevant information with foreign authorities relating to possible violations of Laws Protecting Privacy;

    b. Enabling their Privacy Enforcement Authorities to provide assistance to foreign authorities relating to possible violations of their Laws Protecting Privacy, in particular with regard to obtaining information from persons; obtaining documents or records; or locating or identifying organisations or persons involved or things.

IV. INTERNATIONAL CO-OPERATION

13. Member countries and their Privacy Enforcement Authorities should co-operate with each other, consistent with the provisions of this Recommendation and national law, to address cross-border aspects arising out of the enforcement of Laws Protecting Privacy. Such co-operation may be facilitated by appropriate bilateral or multilateral enforcement arrangements.

A. *Mutual assistance*

14. Privacy Enforcement Authorities requesting assistance from Privacy Enforcement Authorities in other Member countries in procedural, investigative and other matters involved in the enforcement of Laws Protecting Privacy across borders should take the following into account:

    a. Requests for assistance should include sufficient information for the requested Privacy Enforcement Authority to take action. Such information may include a description of the facts underlying the request and the type of assistance sought, as well as an indication of any special precautions that should be taken in the course of fulfilling the request.

    b. Requests for assistance should specify the purpose for which the information requested will be used.

    c. Prior to requesting assistance, a Privacy Enforcement Authority should perform a preliminary inquiry to ensure that the request is consistent with the scope of this Recommendation and does not impose an excessive burden on the requested Privacy Enforcement Authority.

15. The requested Privacy Enforcement Authority may exercise its discretion to decline the request for assistance, or limit or condition its co-operation, in particular where it is outside the scope of this Recommendation, or more generally where it would be inconsistent with domestic laws, or important interests or priorities. The reasons for declining or limiting assistance should be communicated to the requesting authority.

16. Privacy Enforcement Authorities requesting and receiving assistance on enforcement matters should communicate with each other about matters that may assist ongoing investigations.

17. Privacy Enforcement Authorities should, as appropriate, refer complaints or provide notice of possible violations of the Laws Protecting Privacy of other Member countries to the relevant Privacy Enforcement Authority.

18. In providing mutual assistance, Privacy Enforcement Authorities should:

    a. Refrain from using non-public information obtained from another Privacy Enforcement Authority for purposes other than those specified in the request for assistance;

    b. Take appropriate steps to maintain the confidentiality of non-public information exchanged and respect any safeguards requested by the Privacy Enforcement Authority that provided the information;

    c. Co-ordinate their investigations and enforcement activity with that of Privacy Enforcement Authorities in other member countries to promote more effective enforcement and avoid interference with ongoing investigations;

    d. Use their best efforts to resolve any disagreements related to co-operation that may arise.

B. *Engaging in collective initiatives to support mutual assistance*

19. Member countries should designate a national contact point for co-operation and mutual assistance under this Recommendation and

provide this information to the OECD Secretary-General. The designation of the contact point is intended to complement rather than replace other channels for co-operation. Updated information regarding Laws Protecting Privacy should also be provided to the OECD Secretary-General, who will maintain a record of information about the laws and contact points for the benefit of all Member countries.

20. Privacy Enforcement Authorities should share information on enforcement outcomes to improve their collective understanding of how privacy law enforcement is conducted.

21. Member countries should foster the establishment of an informal network of Privacy Enforcement Authorities and other appropriate stakeholders to discuss the practical aspects of privacy law enforcement co-operation, share best practices in addressing cross-border challenges, work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness raising campaigns.

C. *Co-operating with other authorities and stakeholders*

22. Member countries should encourage Privacy Enforcement Authorities to consult with:

    a. Criminal law enforcement authorities to identify how best to co-operate in relation to privacy matters of a criminal nature for the purpose of protecting privacy across borders most effectively;

    b. Privacy officers in public and private organisations and private sector oversight groups on how they could help resolve privacy-related complaints at an early stage with maximum ease and effectiveness;

    c. Civil society and business on their respective roles in facilitating cross-border enforcement of Laws Protecting Privacy, and in particular in helping raise awareness among individuals on how to submit complaints and obtain remedies, with special attention to the cross-border context. Recommendation of the Council on the Protection of Critical Information Infrastructures [C(2008)35][3]

Having regard to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;

Having regard to the Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security [C(2002)131], hereinafter the "Security Guidelines";

Having regard to the Resolution 58/199 adopted by the General Assembly of the United Nations on the creation of a global culture of cyber security and the protection of critical information infrastructures;

Recognizing that the functioning of our economies and societies increasingly relies on information systems and networks that are interconnected and interdependent, domestically and across borders; that a number of those systems and networks are of national critical importance; and that their protection is a priority area for national policy and international cooperation;

Recognizing that in order to improve the protection of domestic and cross-border critical information infrastructures, Member countries need to share their knowledge and experience in developing policies and practices and cooperate more closely between themselves as well as with non Member economies;

Recognizing that the protection of critical information infrastructures requires coordination domestically and across borders with the private sector owners and operators of such infrastructures, hereinafter the "private sector";

On the proposal of the Committee for Information, Computer and Communication Policy:

AGREES that:

For the purposes of this Recommendation, critical information infrastructures, hereinafter "CII", should be understood as referring to those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy;

National CII are identified through a risk assessment process and typically include one or more of the following:

- Information components supporting critical infrastructures, and/or
- Information infrastructures supporting essential components of government business; and/or

3 This Recommendation was developed by the OECD Committee for Information, Computer and Communication Policy (ICCP Committee), and its Working Party on Information Security and Privacy. The Recommendation was adopted by the OECD Council at its 1172nd Session on 30 April 2008.

- Information infrastructures essential to the national economy.

RECOMMENDS that:

Member countries introduce and maintain an effective framework to implement the OECD Security Guidelines in relation to the protection of CII, taking into account the specific policy and operational guidance set out herein;

PART I
PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURES AT THE DOMESTIC LEVEL

Member countries should:

23. Demonstrate government leadership and commitment to protect CII by:
    - Adopting clear policy objectives at the highest level of government.
    - Identifying government agencies and organizations with responsibility and authority to implement these policy objectives.
    - Consulting with private sector owners and operators of CII to establish mutual cooperation for the implementation of these objectives.
    - Ensuring transparency on the delegations of responsibility to government authorities and agencies to facilitate closer co-operation within the government and with the private sector.
    - Systematically reviewing policy and legal frameworks and self-regulatory schemes which may apply to CII, including those addressing cross-border threats, to assess the need to enhance their implementation, to amend them or to develop new instruments.
    - Taking steps, where appropriate, to enhance the security level of components of information system and networks that constitute CII.
24. Manage risks to CII by:
    - Developing a national strategy that gains commitment from all those concerned, including the highest levels of government and the private sector.
    - Taking into consideration interdependencies.
    - Conducting a risk assessment based on the analysis of vulnerabilities and the threats to the CII, in order to protect economies and societies against the impacts of highest national concern.
    - Developing, on the basis of the assessment, and periodically reviewing a national risk management process that sets out the detailed organisation, tools and monitoring mechanisms required to implement the risk management strategy at every level, including:
        - The appropriate organizational structure to provide guidelines and promote good security practices at the national level and to manage and monitor progress, as well as a complete set of processes to ensure preparedness, including prevention, protection, response and recovery from natural and malicious threats.
        - A system of measurement to evaluate and appraise measures in place (including exercises and tests as appropriate) and allow for feedback and continuous update.
    - Developing an incident response capability, such as a computer security incident response team (CERT/CSIRTs), in charge of monitoring, warning, alerting and carrying out recovery measures for CII; and mechanisms to foster closer cooperation and communications among those involved in incident response.
25. Work in partnership with the private sector by:
    - Establishing trusted public-private partnerships with a focus on risk management, incident response and recovery.
    - Enabling mutual and regular exchange of information by establishing information sharing arrangements that acknowledge the sensitivity of certain information.
    - Fostering innovation through public-private research and development projects focused on the improvement of the security of CII and as appropriate, sharing these innovations across borders.

PART II
PROTECTING CRITICAL INFORMATION INFRASTRUCTURES ACROSS BORDERS

Member countries should cooperate among themselves and with the private sector at the strategy, policy and operational levels to ensure the protection of CII against events and circumstances beyond the capacity of individual countries to address alone.

They should in particular proactively engage in bilateral and multilateral cooperation at regional and global levels with a view to:

1. Share knowledge and experience with respect to the development of domestic policies and practices and to models for coordinating with private sector owners and operators of critical information infrastructures.
2. Develop a common understanding of:
    - Risk management applicable to cross-border dependencies and inter-dependencies.
    - Generic vulnerabilities, threats and impacts on the CII, to facilitate collective action to address those that are widespread, such as security flaws and malicious software, as well as to improve risk management strategies and policies.
3. Make available information regarding the national agencies involved in the protection of CII, their roles and responsibilities, to facilitate identification of counterparts and improve the timeliness of cross border action.
4. Acknowledge the value of participation in international or regional networks for watch, warning and incident response, to enable robust information sharing and coordination at the operational level, as well as to better manage crisis in case of an incident developing across borders.
5. Support cross-border collaboration for, and information sharing on, public-private research and development for the protection of CII.

INVITES: Member countries to disseminate this Recommendation throughout the public and private sectors, including governments, businesses and other international organisations to encourage all relevant participants to take the necessary steps for the protection of CII;

Non-Member economies to take account of this Recommendation and collaborate with Member countries in its implementation;

INSTRUCTS the OECD Committee for Information, Computer and Communication Policy to:

Promote the implementation of this Recommendation and review it every five years to foster international co-operation on issues relating to the protection of CII.

ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE

OSCE Ministerial Council Decision No. 3/04 "Combating the Use of the Internet for Terrorist Purposes" (2004)

THE MINISTERIAL COUNCIL,

Recognizing United Nations Security Council resolutions 1373 (2001) and 1566 (2004) as milestones of the international legal framework for the fight against terrorism,

Determined to further intensify efforts in the implementation of existing OSCE commitments on combating terrorism, as reflected in the OSCE Charter on Preventing and Combating Terrorism, Porto Ministerial Council Decision No. 1 on implementing the OSCE commitments and activities on combating terrorism, the Bucharest Plan of Action for Combating Terrorism and the OSCE Strategy to Address Threats to Security and Stability in the Twenty-First Century,

Recalling the Council of Europe Convention on Cybercrime (November 2001), and other relevant works developed in this forum, as well as the results of the Council of Europe Conference on the Challenge of Cybercrime,

Recalling the OSCE Meeting on the Relationship Between Racist, Xenophobic and Anti-Semitic Propaganda on the Internet and Hate Crimes (Paris, 15 and 16 June 2004),

Concerned by the extent of use of the Internet by terrorist organizations:

- To identify and to recruit potential members,
- To collect and transfer funds,
- To organize terrorist acts,
- To incite terrorist acts in particular through the use of propaganda,

Decides that participating States will exchange information on the use of the Internet for terrorist purposes and identify possible strategies to combat this threat, while ensuring respect for international human rights obligations and standards, including those concerning the rights to privacy and freedom of opinion and expression;

Tasks the Secretary General to organize in 2005, in co-operation with Interpol and other interested international organizations, an expert workshop to exchange information on the extent of this threat, as well as on the existing legal framework and institutional tools, and

to consider concrete measures to enhance international co-operation on this issue.

OSCE Ministerial Council Decision No. 7/06 "Countering the Use of the Internet for Terrorist Purposes" (2006)

THE MINISTERIAL COUNCIL,

Recalling its previous decision on this issue (MC.DEC/3/04),

Remaining gravely concerned with the growing use of the Internet for terrorist purposes as outlined in the aforementioned decision and beyond,

Reaffirming in this context the importance of fully respecting the right to freedom of opinion and freedom of expression, which include the freedom to seek, receive and impart information, which are vital to democracy and in fact are strengthened by the Internet (PC.DEC/633 of 11 November 2004) and the rule of law,

Recognizing that United Nations Security Council resolution 1624 (2005) calls upon States to take measures that are necessary and appropriate, and in accordance with their obligations under international law, to prohibit by law incitement to commit a terrorist act or acts and to prevent such conduct,

Reaffirming our commitments under the United Nations Global Counter-Terrorism Strategy, in particular "to coordinate efforts at the international and regional level to counter terrorism in all its forms and manifestations on the Internet" and "to use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard",

Noting the observation in the report by the UN Counter-Terrorism Committee (S/2006/737 of 15 September 2006) that several States reported they are studying the application of the prohibition on incitement in their national legislation to the Internet,

Noting recent developments, in particular the Council of Europe Convention on the Prevention of Terrorism, regarding the obligations of States parties to this Convention to criminalize public provocation to commit a terrorist offence and recruitment and training for terrorism,

Recalling the Council of Europe's Convention on Cybercrime (2001), the only legally binding multilateral instrument that specifically addresses cybercrime by, inter alia providing for a common legal framework for international co-operation between States parties to this Convention in combating cybercrime, and its Additional Protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems,

Recognizing the commitment by the G8 Summit (St. Petersburg, Russian Federation, 16 July 2006) to effectively counter attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists, and in particular noting the role of the G8 24/7 Computer Crime Network for countering criminal conduct in cyberspace,

Recalling the results of the OSCE Special Meeting on the Relationship between Racist, Xenophobic and Anti-Semitic Propaganda on the Internet and Hate Crimes (Paris, 15 and 16 June 2004), as well as the outcomes of the OSCE Expert Workshop on Combating the Use of the Internet for Terrorist Purposes (Vienna, 13 and 14 October 2005) and the OSCE-Council of Europe Expert Workshop on Preventing Terrorism: Fighting Incitement and Related Terrorist Activities (Vienna, 19 and 20 October 2006), and relevant work done by the OSCE Secretariat and institutions, in particular by the Representative on Freedom of the Media and the ODIHR,

Taking into account different national approaches to defining "illegal" and "objectionable" content and different methods of dealing with illegal and objectionable content in cyberspace, such as the possible use of intelligence collected from Internet traffic and content to closing websites of terrorist organizations and their supporters,

Concerned with continued hacker attacks, which though not terrorism related, still demonstrate existing expertise in the field and thus providing a possibility of terrorist cyber attacks against computer systems, affecting the work of critical infrastructures, financial institutions or other vital networks,

1. Decides to intensify action by the OSCE and its participating States, notably by enhancing international co-operation on countering the use of the Internet for terrorist purposes;

2. Calls on participating States to consider taking all appropriate measures to protect vital critical information infrastructures and networks against the threat of cyber attacks;

3. Calls on participating States to consider becoming party to and to implement their obligations under the existing international and regional legal instruments, including the Council of Europe's Conventions on Cybercrime (2001) and

on the Prevention of Terrorism (2005);

4. Encourages participating States to join the G8 24/7 Computer Crime Network and to nominate an appropriate unit/contact person for this network for the purpose of streamlining international law enforcement co-operation on combating the criminal misuse of cyberspace and in criminal cases that involve electronic evidence, as appropriate;

5. Calls on participating States, when requested to deal with content that is illegal under their national legislation and is hosted within their jurisdiction, to take all appropriate action against such content and to co-operate with other interested States, in accordance with their national legislation and the rule of law, and in line with their international obligations, including international human rights law;

6. Invites participating States to increase their monitoring of websites of terrorist/violent extremist organizations and their supporters and to invigorate their exchange of information in the OSCE and other relevant fora on the use of the Internet for terrorist purposes and measures taken to counter it, in line with national legislation, while ensuring respect for international human rights obligations and standards, including those concerning the rights to privacy and freedom of opinion and expression, and the rule of law. Duplication of efforts with ongoing activities in other international fora should be avoided;

7. Recommends participating States to explore the possibility of more active engagement of civil society institutions and the private sector in preventing and countering the use of the Internet for terrorist purposes;

8. Encourages participating States to participate in the May 2007 "OSCE political conference on public-private partnership in countering terrorism" in Vienna that will focus on the vital role the private sector, including businesses, civil society and the media, can play in co-operating with governments to prevent and combat terrorism;

9. Tasks the Secretary General to promote, notably through the OSCE Counter-Terrorism Network, the exchange of information on the threat posed by the use of the Internet for terrorist purposes, including incitement, recruitment, fund raising, training, targeting and planning terrorist acts, and on legislative and other measures taken to counter this threat.

Parliamentary Assembly "Astana" Resolution on Cyber Security and Cyber Crime (2008)

July 1, 2008

10. *Recalling* that in the contemporary world armed conflicts are not the only breeding ground for threats against States and citizens,

11. *Recognizing* the essential role of co-operation between all governments in order to successfully cope with modern security risks,

12. *Underlining* the fact that cyber attacks have become a serious security threat, which cannot be underestimated,

13. *Recognizing* that cyber attacks can be a great challenge to governments, because they may destabilize society, jeopardize the availability of public services and the functioning of vital state infrastructure,

14. *Reiterating* that any country which relies extensively on information and communication technology may fall victim to cyber crime,

15. *Welcoming* the discussions in international fora on how to respond effectively to the abuse of cyber space for criminal and in particular terrorist purposes,

16. *Recognizing* that cyber security and cyber crime have become a matter of substantial concern to inter alia the Council of Europe, the EU, NATO and the UN General Assembly,

17. *Reaffirming* the role of the OSCE as a regional arrangement under Chapter VIII of the UN Charter and a key instrument for early warning, conflict prevention, crisis management and post-conflict rehabilitation in its area,

18. *Reiterating* its concern over the persistence of cyber attacks in various places of the OSCE area,

19. *Recognizing* the previous work done in the OSCE with respect to various aspects of cyber security and cyber crime, and in particular related to terrorist use of the Internet,

20. *Underlining* the urgent need for the international community to increase co-operation and information exchange in the field of cyber security and cyber crime, because only with joint and coordinated efforts is it possible to effectively respond to the threats originating from

cyber space,

21. *Stressing* that the Council of Europe Convention on Cybercrime of 2001 is the only legally binding multilateral instrument specifically addressing computer-related crime, but that it has been ratified by only 22 States,

22. *Welcoming* the discussions and decisions initiated by NATO, the Parliamentary Assembly of the Council of Europe, and elsewhere,

23. *Welcoming* the fact that several OSCE participating States have already developed and adopted countermeasures against various kinds of cyber threats,

24. *Emphasizing* the commitment of OSCE participating States to respect and foster the principles of international law,

The OSCE Parliamentary Assembly:

25. *Expresses* its regret that the international community has not been able to agree on specific countermeasures against cyber threats so far;

26. *Urges* the parliamentarians of the OSCE participating States to intensify their efforts in convincing the parliaments and governments in their countries that threats originating from cyber space are one of the most serious security challenges of present time, which can jeopardize the way of life of modern societies and the whole of civilization;

27. *Urges* governments to condemn cyber attacks on a moral basis, as analogous to trafficking in human beings or to intellectual property piracy, and to create universal rules of conduct in cyber space;

28. *Maintains* that the results of a cyber attack against vital state infrastructure do not differ in nature from those of a conventional aggressive act;

29. *Urges* OSCE participating States and all other members of the international community to consider joining the Council of Europe Convention on Cybercrime and unconditionally follow its provisions;

30. *Urges* OSCE participating States to consider joining also the Council of Europe Convention on the Prevention of Terrorism which offers additional instruments for preventing cyber attacks by terrorist groups and use of the Internet for terrorist purposes;

31. *Draws attention* to the need to revise existing legal acts concerning cyber security and cyber crime and to find supplementary means, including harmonisation of the relevant legislation of States, and to make international co-operation in the field of cyber security and cyber crime more efficient;

32. *Urges* all parties involved to search, in good faith, for negotiated solutions in the field of cyber security and cyber crime in order to achieve a comprehensive and lasting settlement which shall be based on the norms and principles of international law;

33. *Calls upon* all parties to make full use of available mechanisms and formats for dialogue in a constructive spirit;

34. *Supports* all efforts to enhance information exchange on relevant experiences and best practices, involving also relevant actors from the private sector and civil society, and to establish public-private partnerships in this regard;

35. *Encourages* OSCE participating States to develop, adopt and implement national action plans on cyber security and cyber crime;

36. *Recommends* that the OSCE could function as a regional mechanism supporting, coordinating and reviewing the development and implementation of national activities in this field, building on and furthering previous activities related to various aspects of cyber security and cyber crime;

37. *Urges* OSCE participating States to adopt anticipatory measures in order to prevent security incidents, to increase the security awareness of information and communication technology users;

38. *Stresses* the need to analyse the sufficiency of existing measures and to supplement them according to the experience gained;

39. *Welcomes* the proposal to hold a conference or a round-table for OSCE parliamentarians, taking into account and building on previously held OSCE events related to various aspects of cyber security and cyber crime, to gain, through the help of experts, detailed information on all relevant aspects of the issue;

40. *Asks* the representatives of OSCE participating States to forward this resolution to the governments and parliaments of their countries.

THE UNITED NATIONS

Guidelines for the regulation of computerized personal data files (Regulation 44/132 of 5 December 1989)

The General Assembly,

Bearing in mind Commission on Human Rights resolution 1989/43 of 6 March 1989 and Economic and Social Council resolution 1989/78 of 24 May 1989, entitled "Guidelines on the use of computerized personal data files",

1. *Expresses its appreciation* to the Special Rapporteur of the Sub-Commission on Prevention of Discrimination and Protection of Minorities, Mr. Louis Joinet, for his report on the draft guidelines for the regulation of computerized personal data files;[1]

2. *Conveys its thanks* to the Governments that have communicated to the Secretary-General their comments and suggestions on the draft guidelines;[2]

3. *Invites* the Special Rapporteur to submit to the Commission on Human Rights at its forty-sixth session a revised version of the draft guidelines, taking into account, inter alia, those comments and suggestions;

4. *Requests* the Commission on Human Rights to examine the revised draft guidelines and, once it has examined and, if necessary, modified them, to transmit them, through the Economic and Social Council, to the General Assembly at its forty-fifth session for final adoption.

1 E/CN.4/Sub.2/1988/22
2 See A/44/606 and Add. l

Guidelines for the regulation of computerized personal data tiles (Resolution 45/95 of 14 December 1990)

The General Assembly,

Recalling its resolution 44/132 of 15 December 1989,

Bearing in mind Commission on Human Rights resolution 1990/42 of 6 March 1990 and Economic and Social Council resolution 1990/38 of 25 May 1990, entitled "Guidelines on the use of computerized personal files",

1. *Expresses its appreciation* to the Special Rapporteur of the Sub-Commission on Prevention of Discrimination and Protection of Minorities, Mr. Louis Joinet, for his report containing a revised version of the draft guidelines for the regulation of computerized personal data files;[3]

2. *Conveys its thanks* to the Governments that have communicated to the Secretary-General their comments and suggestions4 concerning the previous version of the draft guidelines;[5]

3. *Adopts* the guidelines for the regulation of computerized personal data files in their revised version;

4. *Requests* Governments to take into account those guidelines in their legislation and administrative regulations;

5. *Requests* governmental, intergovernmental and non-governmental organizations to respect those guidelines in carrying out the activities within their field of competence.

3 E/CN.4/1990/72
4 See A/44/606 and Add. 1.
5 E/CN.4/Sub.2/1988/22

Developments in the field of information and telecommunications in the context of international security (Resolution 53/70 of 4 December 1998)

The General Assembly,

Recalling its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of mankind, and additional improvements in the circulation of information in the global community,

Recalling in this connection the approaches and principles outlined at the Information Society and Development Conference, held at Midrand, South Africa, from 13 to 15 May 1996,

Taking note of the results of the Ministerial Conference on Terrorism, held in Paris on 30 July 1996, and of the recommendations it made,[6]

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Expressing concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States,

Considering that it is necessary to prevent the misuse or exploitation of information resources or technologies for criminal or terrorist purposes,

1. *Calls upon* Member States to promote at multilateral levels the consideration of existing and potential threats in the field of information security;

2. *Invites* all Member States to inform the Secretary-General of their views and assessments on the following questions:

   (a) General appreciation of the issues of information security;

   (b) Definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources;

   (c) Advisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality;

3. *Requests* the Secretary-General to submit a report to the General Assembly at its fifty-fourth session;

4. *Decides* to include in the provisional agenda of its fifty-fourth session an item entitled

"Developments in the field of information and telecommunications in the context of international security".

6 See A/51/261, annex.

Developments in the field of information and telecommunications in the context of international security (Resolution 54/49 of 1 December 1999)

The General Assembly,

Recalling its resolution 53/70 of 4 December 1998,

Recalling also its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of mankind and additional improvements in the circulation of information in the global community,

Recalling in this connection the approaches and principles outlined at the Information Society and Development Conference, held at Midrand, South Africa, from 13 to 15 May 1996,

Taking note of the results of the Ministerial Conference on Terrorism, held in Paris on 30 July 1996, and of the recommendations it made,[7]

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Expressing concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States in both civilian and military fields,

Considering that it is necessary to prevent the misuse or exploitation of information resources or technologies for criminal or terrorist purposes,

Noting the contribution of those Member States that have submitted their assessments on issues of information security to the Secretary-General pursuant to paragraphs 1 to 3 of resolution 53/70,

Taking note of the report of the Secretary-General containing those assessments,[8]

Welcoming the timely initiative taken by the Secretariat and the United Nations Institute for Disarmament Research in convening an international meeting of experts at Geneva in August 1999 on developments in the field of information and telecommunications in the context of international security,

Considering that the assessments of Member States contained in the report of the Secretary-General and the international meeting of experts have contributed to a better understanding of the substance of issues of international information security, related notions and possible measures to limit the threats emerging in this field,

1. *Calls upon* Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security;

2. *Invites* all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

   (a) General appreciation of the issues of information security;

   (b) Definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources;

   (c) Advisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality;

3. *Requests* the Secretary-General to submit a report to the General Assembly at its fifty-fifth session;

4. *Decides* to include in the provisional agenda of its 55th session the item entitled "Developments in the field of information and telecommunications in the context of international security".

7 A/51/261, annex.

8 A/54/213.

Developments in the field of information and telecommunications in the context of international security (Resolution 55/28 of 20 November 2000)

The General Assembly,

Recalling its resolutions 53/70 of 4 December 1998 and 54/49 of 1 December 1999,

Recalling also its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of mankind and additional improvements in the circulation of information in the global community,

Recalling in this connection the approaches and principles outlined at the Information Society and Development Conference, held at Midrand, South Africa, from 13 to 15 May 1996,

Bearing in mind the results of the Ministerial Conference on Terrorism, held in

Paris on 30 July 1996, and the recommendations it made,[9]

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Expressing concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States in both civil and military fields,

Noting the contribution of those Member States that have submitted their assessments on issues of information security to the Secretary-General pursuant to paragraphs 1 to 3 of resolutions 53/70 and 54/49,

Taking note of the reports of the Secretary-General containing those assessments,[10]

Welcoming the initiative taken by the Secretariat and the United Nations Institute for Disarmament Research in convening an international meeting of experts at Geneva in August 1999 on developments in the field of information and telecommunications in the context of international security, as well as its results,

Considering that the assessments of the Member States contained in the reports of the Secretary-General and the international meeting of experts have contributed to a better understanding of the substance of issues of international information security and related notions,

1. *Calls upon* Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field;

2. *Considers* that the purpose of such measures could be served through the examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

3. *Invites* all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

   (a) General appreciation of the issues of information security;

   (b) Definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources;

   (c) The content of the concepts mentioned in paragraph 2 of the present resolution;

4. *Requests* the Secretary-General to submit a report based on replies received from Member States to the General Assembly at its fifty-sixth

9 See A/51/261, annex.

10 A/54/213 and A/55/140 and Corr.1 and Add.1.

session;

5. *Decides* to include in the provisional agenda of its fifty-sixth session the item entitled "Developments in the field of information and telecommunications in the context of international security".

Combating the criminal misuse of information technologies (Resolution 55/63 of 4 December 2000)

The General Assembly,

Recalling the United Nations Millennium Declaration,[11] in which Member States resolved to ensure that the benefits of new technologies, especially information and communication technologies, in conformity with recommendations contained in the Ministerial Declaration of the high-level segment of the substantive session of 2000 of the Economic and Social Council,[12] are available to all,

Recalling also its resolution 45/121 of 14 December 1990, in which it endorsed the recommendations of the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,[13] and noting in particular the resolution on computer-related crimes,[14] in which the Eighth Congress called upon States to intensify their efforts to combat computer-related abuses more effectively,

Emphasizing the contributions that the United Nations, in particular the Commission on Crime Prevention and Criminal Justice, can make in the promotion of more efficient and effective law enforcement and administration of justice and of the highest standards of fairness and human dignity,

Recognizing that the free flow of information can promote economic and social development, education and democratic governance,

Noting significant advancements in the development and application of information technologies and means of telecommunication,

Expressing concern that technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies,

Noting that reliance on information technologies, while it may vary from State to State, has resulted

11 See resolution 55/2.
12 See A/55/3, chap. III. For the final text, see Official Records of the General Assembly, Fifty-fifth Session, Supplement No. 3.
13 Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August–7 September 1990: report prepared by the Secretariat (United Nations publication, Sales No. E.91.IV.2), chap I.
14 Ibid., sect. C, resolution 9.

in a substantial increase in global cooperation and coordination, with the result that the criminal misuse of information technologies may have a grave impact on all States,

Recognizing that gaps in the access to and use of information technologies by States can diminish the effectiveness of international cooperation in combating the criminal misuse of information technologies, and noting the need to facilitate the transfer of information technologies, in particular to developing countries,

Noting the necessity of preventing the criminal misuse of information technologies,

Recognizing the need for cooperation between States and private industry in combating the criminal misuse of information technologies,

Underlining the need for enhanced coordination and cooperation among States in combating the criminal misuse of information technologies, and, in this context, stressing the role that can be played by both the United Nations and regional organizations,

Welcoming the work of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,[15]

Noting the work of the Committee of Experts on Crime in Cyberspace of the Council of Europe on a draft convention on cybercrime, the principles agreed to by the Ministers of Justice and the Interior of the Group of Eight in Washington, D.C., on 10 December 1997, which were endorsed by the heads of State of the Group of Eight in Birmingham, United Kingdom of Great Britain and Northern Ireland, on 17 May 1998, the work of the Conference of the Group of Eight on a dialogue between government and industry on safety and confidence in cyberspace, held in Paris from 15 to 17 May 2000, and the recommendations approved on 3 March 2000 by the Third Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas, convened in San José, Costa Rica, from 1 to 3 March 2000 within the framework of the Organization of American States,[16]

1. *Notes with appreciation* the efforts of the abovementioned bodies to prevent the criminal misuse of information technologies, and also notes the value of, inter alia, the following measures to combat such misuse:

   (a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;

   (b) Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;

   (c) Information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies;

   (d) Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;

   (e) Legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized;

   (f) Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;

   (g) Mutual assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such cases;

   (h) The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies;

   (i) To the extent practicable, information technologies should be designed to help to prevent and detect criminal misuse, trace criminals and collect evidence;

   (j) The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse;

2. *Invites* States to take into account the abovementioned measures in their efforts to combat the criminal misuse of information technologies;

3. *Decides* to maintain the question of the criminal misuse of information technologies on the agenda of its fifty-sixth session, as part of the

15 See Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10–17 April 2000: report prepared by the Secretariat (United Nations publication, Sales No. E.00.IV.8).

16 See REMJA-III/doc.14/00 rev. 2, chap. IV.

item entitled "Crime prevention and criminal justice".

Developments in the field of information and telecommunications in the context of international security (Resolution 56/19 of 29 November 2001)

The General Assembly,

Recalling its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999 and 55/28 of 20 November 2000,

Recalling also its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of mankind and additional improvements in the circulation of information in the global community,

Recalling, in this connection, the approaches and principles outlined at the

Information Society and Development Conference, held at Midrand, South Africa, from 13 to 15 May 1996,

Bearing in mind the results of the Ministerial Conference on Terrorism, held in

Paris on 30 July 1996, and the recommendations that it made,[17]

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Expressing concern that these technologies and

17 See A/51/261, annex.

means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States in both civil and military fields,

Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

Noting the contribution of those Member States that have submitted their assessments on issues of information security to the Secretary-General pursuant to paragraphs 1 to 3 of resolutions 53/70, 54/49 and 55/28,

Taking note of the reports of the Secretary-General containing those assessments,[18]

Welcoming the initiative taken by the Secretariat and the United Nations Institute for Disarmament Research in convening an international meeting of experts at Geneva in August 1999 on developments in the field of information and telecommunications in the context of international security, as well as its results,

Considering that the assessments of the Member States contained in the reports of the Secretary-General and the international meeting of experts have contributed to a better understanding of the substance of issues of international information security and related notions,

1. *Calls upon* Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field, consistent with the need to preserve the free flow of information;

2. *Considers* that the purpose of such measures could be served through the examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

3. *Invites* all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

   (a) General appreciation of the issues of information security;

   (b) Definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources;

   (c) The content of the concepts mentioned in paragraph 2 of the present resolution;

4. *Requests* the Secretary-General to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them, and to conduct a study on the concepts referred to in paragraph 2 of the present resolution, with the assistance of a group of governmental experts, to be established in 2004, appointed by him on the basis of equitable geographical distribution and with the help of Member States in a position to render such assistance, and to submit a report on the outcome of the study to the General Assembly at its sixtieth session;

5. *Decides* to include in the provisional agenda of its fifty-seventh session the item entitled "Developments in the field of information and telecommunications in the context of international security"

18 A/54/213, A/55/140 and Corr.1 and Add.1, and A/56/164 and Add.1.

Combating the criminal misuse of information technologies (Resolution 56/121 of 19 December 2001)

The General Assembly,

Recalling the United Nations Millennium Declaration,[19] in which Member States resolved to ensure that the benefits of new technologies, especially information and communications technologies, in conformity with the recommendations contained in the ministerial declaration of the high-level segment of the substantive session of 2000 of the Economic and Social Council,[20] are available to all, and its resolution 55/63 of 4 December 2000, in which it invited Member States to take into account measures to combat the criminal misuse of information technologies,

Recognizing that the free flow of information can promote economic and social development, education and democratic governance,

Noting the significant advancements in the development and application of information technologies and means of telecommunication,

Expressing concern that technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies,

Noting that reliance on information technologies, while it may vary from State to State, has resulted in a substantial increase in global cooperation and coordination, with the result that the criminal misuse of information technologies may have a grave impact on all States,

Recognizing that gaps in the access to and use of information technologies by States can diminish the effectiveness of international cooperation in combating the criminal misuse of information technologies, and recognizing also the need to facilitate the transfer of information technologies, in particular to developing countries,

Noting the necessity of preventing the criminal misuse of information technologies,

Recognizing the need for cooperation between States and the private sector in combating the criminal misuse of information technologies,

Underlining the need for enhanced coordination and cooperation among States in combating the criminal misuse of information technologies, and, in this context, stressing the role that can be played by the United Nations and other international and regional organizations,

Welcoming the work of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,

Recognizing with appreciation the work of the Commission on Crime Prevention and Criminal Justice at its ninth and tenth sessions and the subsequent preparation of a plan of action against high-technology and computer-related crime, which recognizes, inter alia, the need for effective law enforcement and the need to maintain effective protections for privacy and other related basic rights, as well as the need to take into account ongoing work in other forums,[21]

Noting the work of international and regional organizations in combating high technology crime, including the work of the Council of Europe in elaborating the Convention on Cybercrime,[22] as well as the work of those organizations in promoting dialogue between government and the private sector on safety and confidence in cyberspace,

1. *Invites* Member States, when developing national law, policy and practice to combat the criminal misuse of information technologies, to take into account, as appropriate, the work and achievements of the Commission on Crime Prevention and Criminal Justice and of other international and regional organizations;

2. *Takes note* of the value of the measures set forth in its resolution 55/63, and again invites Member States to take them into account in their efforts to combat the criminal misuse of information technologies;

3. *Decides* to defer consideration of this subject, pending work envisioned in the plan of action against high-technology and computer-related crime of the Commission on Crime Prevention and Criminal Justice.

19 See resolution 55/2.

20 See Official Records of the General Assembly, Fifty-fifth Session, Supplement No. 3 (A/55/3/Rev.1), chap. III, para. 17.

21 See Official Records of the Economic and Social Council, 2001, Supplement No. 10 (E/2001/30/Rev.1), part two, chap. I.

22 Council of Europe, European Treaty Series, No. 185.

Developments in the field of information and telecommunications in the context of international security (Resolution 57/53 of 22 November 2002)

The General Assembly,

Recalling its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000 and 56/19 of 29 November 2001,

Recalling also its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community,

Recalling, in this connection, the approaches and principles outlined at the Information Society and Development Conference, held in Midrand, South Africa, from 13 to 15 May 1996,

Bearing in mind the results of the Ministerial Conference on Terrorism, held in Paris on 30 July 1996, and the recommendations that it made,[23]

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Expressing concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields,

Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

Noting the contribution of those Member States that have submitted their assessments on issues of information security to the Secretary-General pursuant to paragraphs 1 to 3 of resolutions 53/70, 54/49, 55/28 and 56/19,

Taking note of the reports of the Secretary-General containing those assessments,[24]

Welcoming the initiative taken by the Secretariat and the United Nations Institute for Disarmament Research in convening an international meeting of experts in Geneva in August 1999 on developments in the field of information and telecommunications in the context of international security, as well as its results,

Considering that the assessments of the Member States contained in the reports of the Secretary-General and the international meeting of experts have contributed to a better understanding of the substance of issues of international information security and related notions,

Confirming the request to the Secretary-General contained in paragraph 4 of its resolution 56/19,

1. *Calls upon* Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field, consistent with the need to preserve the free flow of information;

2. *Considers* that the purpose of such measures could be served through the examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

3. *Invites* all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

   (a) General appreciation of the issues of information security;

   (b) Definition of basic notions related to information security, including unauthorized

23 See A/51/261, annex.

24 A/54/213, A/55/140 and Corr.1 and Add.1, A/56/164 and Add.1 and A/57/166 and Add.1.

interference with or misuse of information and telecommunications systems and information resources;

(c) The content of the concepts mentioned in paragraph 2 of the present resolution;

4. *Requests* the Secretary-General to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them, and to conduct a study on the concepts referred to in paragraph 2 of the present resolution, with the assistance of a group of governmental experts, to be established in 2004, appointed by him on the basis of equitable geographical distribution and with the help of Member States in a position to render such assistance, and to submit a report on the outcome of the study to the General Assembly at its sixtieth session;

5. *Decides* to include in the provisional agenda of its fifty-eighth session the item entitled "Developments in the field of information and telecommunications in the context of international security".

Creation of a global culture of cyber security (Resolution 57/239 of 20 December 2002)

The General Assembly,

Noting the growing dependence of Governments, businesses, other organizations and individual users on information technologies for the provision of essential goods and services, the conduct of business and the exchange of information,

Recognizing that the need for cybersecurity increases as countries increase their participation in the information society,

Recalling its resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on establishing the legal basis for combating the criminal misuse of information technologies,

*Recalling a*lso its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001 and 57/53 of 22 November 2002 on developments in the field of information and telecommunications in the context of international security,

Aware that effective cybersecurity is not merely a matter of government or law enforcement practices, but must be addressed through prevention and supported throughout society,

Aware also that technology alone cannot ensure cybersecurity and that priority must be given to cybersecurity planning and management throughout society,

Recognizing that, in a manner appropriate to their roles, government, business, other organizations, and individual owners and users of information technologies must be aware of relevant cybersecurity risks and preventive measures and must assume responsibility for and take steps to enhance the security of these information technologies,

Recognizing also that gaps in access to and the use of information technologies by States can diminish the effectiveness of international cooperation in combating the criminal misuse of information technology and in creating a global culture of cybersecurity, and noting the need to facilitate the transfer of information technologies, in particular to developing countries,

Recognizing further the importance of international cooperation for achieving cybersecurity through

the support of national efforts aimed at the enhancement of human capacity, increased learning and employment opportunities, improved public services and better quality of life by taking advantage of advanced, reliable and secure information and communication technologies and networks and by promoting universal access,

Noting that, as a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities which raise new security issues for all,

Noting also the work of relevant international and regional organizations on enhancing cybersecurity and the security of information technologies,

1. *Takes note* of the elements annexed to the present resolution, with a view to creating a global culture of cybersecurity;
2. *Invites* all relevant international organizations to consider, inter alia, these elements for the creation of such a culture in any future work on cybersecurity;
3. *Invites* Member States to take into account these elements, inter alia, in their efforts to develop throughout their societies a culture of cybersecurity in the application and use of information technologies;
4. *Invites* Member States and all relevant international organizations to take, inter alia, these elements and the need for a global culture of cybersecurity into account in their preparations for the World Summit on the Information Society, to be held at Geneva from 10 to 12 December 2003 and at Tunis in 2005;
5. *Stresses* the necessity to facilitate the transfer of information technology and capacity-building to developing countries, in order to help them to take measures in cybersecurity. 78th plenary meeting 20 December 2002

Annex

Elements for creating a global culture of cybersecurity

Rapid advances in information technology have changed the way Governments, businesses, other organizations and individual users who develop, own, provide, manage, service and use information systems and networks ("participants") must approach cybersecurity. A global culture of cybersecurity will require that all participants address the following nine complementary elements:

(a) *Awareness*. Participants should be aware of the need for security of information systems and networks and what they can do to enhance security;

(b) *Responsibility*. Participants are responsible for the security of information systems and networks in a manner appropriate to their individual roles. They should review their own policies, practices, measures and procedures regularly, and should assess whether they are appropriate to their environment;

(c) *Response*. Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective cooperation to prevent, detect and respond to security incidents. This may involve cross-border information-sharing and cooperation;

(d) *Ethics*. Given the pervasiveness of information systems and networks in modern societies, participants need to respect the legitimate interests of others and recognize that their action or inaction may harm others;

(e) *Democracy*. Security should be implemented in a manner consistent with the values recognized by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency;

(f) *Risk assessment*. All participants should conduct periodic risk assessments that identify threats and vulnerabilities; are sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications; allow determination of the acceptable level of risk; and assist in the selection of appropriate controls to manage the risk of potential harm to information systems and networks in the light of the nature and importance of the information to be protected;

(g) *Security design and implementation*. Participants should incorporate security as an essential element in the planning and design, operation and use of information systems and networks;

(h) *Security management*. Participants should adopt a comprehensive approach to security management based on risk assessment that is dy-

namic, encompassing all levels of participants' activities and all aspects of their operations;

(i) *Reassessment*. Participants should review and reassess the security of information systems and networks and should make appropriate modifications to security policies, practices, measures and procedures that include addressing new and changing threats and vulnerabilities.

Developments in the field of information and telecommunications in the context of international security (Resolution 58/32 of 8 December 2003)

The General Assembly,

Recalling its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001 and 57/53 of 22 November 2002,

Recalling also its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community,

Recalling, in this connection, the approaches and principles outlined at the Information Society and Development Conference, held in Midrand, South Africa, from 13 to 15 May 1996,

Bearing in mind the results of the Ministerial Conference on Terrorism, held in Paris on 30 July 1996, and the recommendations that it made,[25]

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Expressing its concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining in-

25 See A/51/261, annex.

ternational stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields,

Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

Noting the contribution of those Member States that have submitted their assessments on issues of information security to the Secretary-General pursuant to paragraphs 1 to 3 of resolutions 53/70, 54/49, 55/28, 56/19 and 57/53,

Taking note of the reports of the Secretary-General containing those assessments,[26]

Welcoming the initiative taken by the Secretariat and the United Nations Institute for Disarmament Research in convening an international meeting of experts in Geneva in August 1999 on developments in the field of information and telecommunications in the context of international security, as well as its results,

Considering that the assessments of the Member States contained in the reports of the Secretary-General and the international meeting of experts have contributed to a better understanding of the substance of issues of international information security and related notions,

Confirming the request to the Secretary-General contained in paragraph 4 of its resolutions 56/19 and 57/53,

1. *Calls upon* Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field, consistent with the need to preserve the free flow of information;

2. *Considers* that the purpose of such measures could be served through the examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

3. *Invites* all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

   (a) General appreciation of the issues of information security;

   (b) Definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources;

   (c) The content of the concepts mentioned in paragraph 2 of the present resolution;

4. *Requests* the Secretary-General to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them, and to conduct a study on the concepts referred to in paragraph 2 of the present resolution, with the assistance of a group of governmental experts, to be established in 2004, appointed by him on the basis of equitable geographical distribution and with the help of Member States in a position to render such assistance, and to submit a report on the outcome of the study to the General Assembly at its sixtieth session;

5. *Decides* to include in the provisional agenda of its fifty-ninth session the item entitled "Developments in the field of information and telecommunications in the context of international security".

26 A/54/213, A/55/140 and Corr.1 and Add.1, A/56/164 and Add.1, A/57/166 and Add.1 and A/58/373.

Creation of a global culture of cyber security and the protection of critical information infrastructures (Resolution 58/199 of 23 December 2003)

The General Assembly,

Recalling its resolutions 57/239 of 20 December 2002 on the creation of a global culture of cybersecurity, 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on establishing the legal basis for combating the criminal misuse of information technologies, and 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001 and 57/53 of 22 November 2002 on developments in the field of information and telecommunications in the context of international security,

Recognizing the growing importance of information technologies for the promotion of socio-economic development and the provision of essential goods and services, the conduct of business and the exchange of information for Governments, businesses, other organizations and individual users,

Noting the increasing links among most countries' critical infrastructures — such as those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health — and the critical information infrastructures that increasingly interconnect and affect their operations,

Recognizing that each country will determine its own critical information infrastructures,

Recognizing also that this growing technological interdependence relies on a complex network of critical information infrastructure components,

Noting that, as a result of increasing interconnectivity, critical information infrastructures are now exposed to a growing number and a wider variety of threats and vulnerabilities that raise new security concerns,

Noting also that effective critical infrastructure protection includes, inter alia, identifying threats to and reducing the vulnerability of critical information infrastructures, minimizing damage and recovery time in the event of damage or attack, and identifying the cause of damage or the source of attack,

Recognizing that effective protection requires communication and cooperation nationally and internationally among all stakeholders and that national efforts should be supported by effective, substantive international and regional cooperation among stakeholders,*Recognizing also* that gaps in access to and the use of information technologies by States can diminish the effectiveness of cooperation in combating the criminal misuse of information technology and in creating a global culture of cyber security, and noting the need to facilitate the transfer of information technologies, in particular to developing countries,

Recognizing further the importance of international cooperation for achieving cyber security and the protection of critical information infrastructures through the support of national efforts aimed at the enhancement of human capacity, increased learning and employment opportunities, improved public services and better quality of life by taking advantage of advanced, reliable and secure information and communication technologies and networks and by promoting universal access,

Noting the work of relevant international and regional organizations on enhancing the security of critical information infrastructures,

Recognizing that efforts to protect critical information infrastructures should be undertaken with due regard for applicable national laws concerning privacy protection and other relevant legislation,

1. *Takes note* of the elements set out in the annex to the present resolution for protecting critical information infrastructures;

2. *Invites* all relevant international organizations, including relevant United Nations bodies, to consider, as appropriate, inter alia, these elements for protecting critical information infrastructures in any future work on cyber security or critical infrastructure protection;

3. *Invites* Member States to consider, inter alia, these elements in developing their strategies for reducing risks to critical information infrastructures, in accordance with national laws and regulations;

4. *Invites* Member States and all relevant international organizations to take, inter alia, these elements and the need for critical information infrastructure protection into account in their preparations for the second phase of the World Summit on the Information Society, to be held in Tunis from 16 to 18 November 2005;

5. *Encourages* Member States and relevant regional and international organizations that have developed strategies to deal with cyber security and the protection of critical information infrastructures to share their best practices and measures that could assist other Member States in their efforts to facilitate the achievement of cyber security;

6. *Stresses* the necessity for enhanced efforts to close the digital divide, to achieve universal access to information and communication technologies and to protect critical information infrastructures by facilitating the transfer of information technology and capacity-building, in particular to developing countries, especially the least developed countries, so that all States may benefit fully from information and communication technologies for their socio-economic development.

Annex: Elements for protecting critical information infrastructures

1. Have emergency warning networks regarding cyber-vulnerabilities, threats and incidents.

2. Raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play in protecting them.

3. Examine infrastructures and identify interdependencies among them, thereby enhancing the protection of such infrastructures.

4. Promote partnerships among stakeholders, both public and private, to share and analyze critical infrastructure information in order to prevent, investigate and respond to damage to or attacks on such infrastructures.

5. Create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.

6. Ensure that data availability policies take into account the need to protect critical information infrastructures.

7. Facilitate the tracing of attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other States.

8. Conduct training and exercises to enhance response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack, and encourage stakeholders to engage in similar activities.

9. Have adequate substantive and procedural laws and trained personnel to enable States to investigate and prosecute attacks on critical information infrastructures and to coordinate such investigations with other States, as appropriate.

10. Engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analyzing information regarding vulnerabilities, threats and incidents and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.

11. Promote national and international research and development and encourage the application of security technologies that meet international standards.

Developments in the field of information and telecommunications in the context of international security (Resolution 59/61 of 3 December 2004)

The General Assembly,

Recalling its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002 and 58/32 of 8 December 2003,

Recalling also its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community,

Recalling, in this connection, the approaches and principles outlined at the Information Society and Development Conference, held in Midrand, South Africa, from 13 to 15 May 1996,

Bearing in mind the results of the Ministerial Conference on Terrorism, held in Paris on 30 July 1996, and the recommendations that it made,[27]

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Expressing its concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields,

Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

Noting the contribution of those Member States that have submitted their assessments on issues of information security to the Secretary-General pursuant to paragraphs 1 to 3 of resolutions 53/70, 54/49, 55/28, 56/19, 57/53 and 58/32,

Taking note of the reports of the Secretary-General containing those assessments,[28]

Welcoming the initiative taken by the Secretariat and the United Nations Institute for Disarmament Research in convening an international meeting of experts in Geneva in August 1999 on developments in the field of information and telecommunications in the context of international security, as well as its results,

Considering that the assessments of the Member States contained in the reports of the Secretary-General and the international meeting of experts have contributed to a better understanding of the substance of issues of international information security and related notions,

1. *Calls upon* Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field, consistent with the need to preserve the free flow of information;

2. *Considers* that the purpose of such measures could be served through the examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

3. *Invites* all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

   (a) General appreciation of the issues of information security;

   (b) Definition of basic notions related to information security, including unauthorized interference with or misuse of information

27 See A/51/261, annex.

28 A/54/213, A/55/140 and Corr.1 and Add.1, A/56/164 and Add.1, A/57/166 and Add.1, A/58/373 and A/59/116 and Add.1.

and telecommunications systems and information resources;

(c) The content of the concepts mentioned in paragraph 2 above;

4. *Notes with satisfaction* that the Secretary-General is considering existing and potential threats in the sphere of information security and possible cooperative measures to address them, and is conducting a study on the concepts referred to in paragraph 2 above, with the assistance of the group of governmental experts, established in 2004 pursuant to resolution 58/32, and will submit a report on the outcome of the study to the General Assembly at its sixtieth session;

5. *Also notes with satisfaction* that the group of governmental experts established by the Secretary-General held its first session from 12 to 16 July 2004 in New York and that it intends to convene two more sessions in 2005 to fulfil its mandate specified in resolution 58/32;

6. *Decides* to include in the provisional agenda of its sixtieth session the item entitled "Developments in the field of information and telecommunications in the context of international security".

Developments in the field of information and telecommunications in the context of international security (Resolution 60/45 of 8 December 2005)

The General Assembly,

Recalling its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, and 59/61 of 3 December 2004,

Recalling also its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community,

Recalling, in this connection, the approaches and principles outlined at the Information Society and Development Conference, held in Midrand, South Africa, from 13 to 15 May 1996,

Bearing in mind the results of the Ministerial Conference on Terrorism, held in Paris on 30 July 1996, and the recommendations that it made,[29]

Bearing in mind also the results of the first phase of the World Summit on the Information Society, held in Geneva from 10 to 12 December 2003,[30]

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that opti-

29 See A/51/261, annex.
30 See A/C.2/59/3.

mum effectiveness is enhanced by broad international cooperation,

Expressing its concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields,

Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

Noting the contribution of those Member States that have submitted their assessments on issues of information security to the Secretary-General pursuant to paragraphs 1 to 3 of resolutions 53/70, 54/49, 55/28, 56/19, 57/53, 58/32 and 59/61,

Taking note of the reports of the Secretary-General containing those assessments,[31]

Welcoming the initiative taken by the Secretariat and the United Nations Institute for Disarmament Research in convening an international meeting of experts in Geneva in August 1999 on developments in the field of information and telecommunications in the context of international security, as well as its results,

Considering that the assessments of the Member States contained in the reports of the Secretary-General and the international meeting of experts have contributed to a better understanding of the substance of issues of international information security and related notions,

Bearing in mind that the Secretary-General, in fulfilment of resolution 58/32, established in 2004 a group of governmental experts, which, in accordance with its mandate, considered existing and potential threats in the sphere of information security and possible cooperative measures to address them and conducted a study on relevant international concepts aimed at strengthening the security of global information and telecommunications systems,

Taking note of the report of the Secretary-General on the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, prepared on the basis of the results of the Group's work,[32]

1. *Calls upon* Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field, consistent with the need to preserve the free flow of information;

2. *Considers* that the purpose of such measures could be served through the examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

3. *Invites* all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

   (a) General appreciation of the issues of information security;

   (b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

   (c) The content of the concepts mentioned in paragraph 2 above;

   (d) Possible measures that could be taken by the international community to strengthen information security at the global level;

4. *Requests* the Secretary-General, with the assistance of a group of governmental experts, to be established in 2009 on the basis of equitable geographical distribution, to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as the concepts referred to in paragraph 2 above, and to submit a report on the results of this study to the General Assembly at its sixty-fifth session;

5. *Decides* to include in the provisional agenda of its sixty-first session the item entitled "Developments in the field of information and telecommunications in the context of international security".

31 A/54/213, A/55/140 and Corr.1 and Add.1, A/56/164 and Add.1, A/57/166 and Add.1, A/58/373, A/59/116 and Add.1 and A/60/95 and Add.1.

32 A/60/202.

Developments in the field of information and telecommunications in the context of international security (Resolution 61/54 of 6 December 2006)

The General Assembly,

Recalling its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004 and 60/45 of 8 December 2005,

Recalling also its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community,

Recalling, in this connection, the approaches and principles outlined at the Information Society and Development Conference, held in Midrand, South Africa, from 13 to 15 May 1996,

Bearing in mind the results of the Ministerial Conference on Terrorism, held in Paris on 30 July 1996, and the recommendations that it made,[33]

Bearing in mind also the results of the World Summit on the Information Society, held in Geneva from 10 to 12 December 2003 (first phase) and in Tunis from 16 to 18 November 2005 (second phase),[34]

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Expressing its concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields,

Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

Noting the contribution of those Member States that have submitted their assessments on issues of information security to the Secretary-General pursuant to paragraphs 1 to 3 of resolutions 53/70, 54/49, 55/28, 56/19, 57/53, 58/32, 59/61 and 60/45,

Taking note of the reports of the Secretary-General containing those assessments,[35]

Welcoming the initiative taken by the Secretariat and the United Nations Institute for Disarmament Research in convening an international meeting of experts in Geneva in August 1999 on developments in the field of information and telecommunications in the context of international security, as well as its results,

Considering that the assessments of the Member States contained in the reports of the Secretary-General and the international meeting of experts have contributed to a better understanding of the substance of issues of international information security and related notions,

Bearing in mind that the Secretary-General, in fulfilment of resolution 58/32, established in 2004 a group of governmental experts, which, in accordance with its mandate, considered existing and potential threats in the sphere of information security and possible cooperative measures to address them and conducted a study on relevant international concepts aimed at strengthening the security of global information and telecommunications systems,

Taking note of the report of the Secretary-General on the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, prepared on the basis of the results of the Group's

33 See A/51/261, annex.
34 See A/C.2/59/3 and A/60/687.
35 A/54/213, A/55/140 and Corr.1 and Add.1, A/56/164 and Add.1, A/57/166 and Add.1, A/58/373, A/59/116 and Add.1, A/60/95 and Add.1 and A/61/161.

work,[36]

1. *Calls upon* Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field, consistent with the need to preserve the free flow of information;

2. *Considers* that the purpose of such measures could be served through the examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

3. *Invites* all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

   (a) General appreciation of the issues of information security;

   (b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

   (c) The content of the concepts mentioned in paragraph 2 above;

   (d) Possible measures that could be taken by the international community to strengthen information security at the global level;

4. *Requests* the Secretary-General, with the assistance of a group of governmental experts, to be established in 2009 on the basis of equitable geographical distribution, to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as the concepts referred to in paragraph 2 above, and to submit a report on the results of this study to the General Assembly at its sixty-fifth session;

5. *Decides* to include in the provisional agenda of its sixty-second session the item entitled "Developments in the field of information and telecommunications in the context of international security".

36 A/60/202.

Developments in the field of information and telecommunications in the context of international security (Resolution 62/17 of 5 December 2007)

The General Assembly,

Recalling its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005 and 61/54 of 6 December 2006,

Recalling also its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community,

Recalling, in this connection, the approaches and principles outlined at the Information Society and Development Conference, held in Midrand, South Africa, from 13 to 15 May 1996,

Bearing in mind the results of the Ministerial Conference on Terrorism, held in Paris on 30 July 1996, and the recommendations that it made,[37]

Bearing in mind also the results of the World Summit on the Information Society, held in Geneva from 10 to 12 December 2003 (first phase) and in Tunis from 16 to 18 November 2005 (second phase),[38]

Noting that the dissemination and use of informa-

37 See A/51/261, annex.
38 See A/C.2/59/3 and A/60/687.

tion technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Expressing its concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields,

Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

Noting the contribution of those Member States that have submitted their assessments on issues of information security to the Secretary-General pursuant to paragraphs 1 to 3 of resolutions 53/70, 54/49, 55/28, 56/19, 57/53, 58/32, 59/61, 60/45 and 61/54,

Taking note of the reports of the Secretary-General containing those assessments,[39]

Welcoming the initiative taken by the Secretariat and the United Nations Institute for Disarmament Research in convening an international meeting of experts in Geneva in August 1999 on developments in the field of information and telecommunications in the context of international security, as well as its results,

Considering that the assessments of the Member States contained in the reports of the Secretary-General and the international meeting of experts have contributed to a better understanding of the substance of issues of international information security and related notions,

Bearing in mind that the Secretary-General, in fulfilment of resolution 58/32, established in 2004 a group of governmental experts, which, in accordance with its mandate, considered existing and potential threats in the sphere of information security and possible cooperative measures to address them and conducted a study on relevant international concepts aimed at strengthening the security of global information and telecommunications systems,

Taking note of the report of the Secretary-General on the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, prepared on the basis of the results of the Group's work,[40]

1. *Calls upon* Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field, consistent with the need to preserve the free flow of information;

2. *Considers* that the purpose of such measures could be served through the examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

3. *Invites* all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

   (a) General appreciation of the issues of information security;

   (b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

   (c) The content of the concepts mentioned in paragraph 2 above;

   (d) Possible measures that could be taken by the international community to strengthen information security at the global level;

4. *Requests* the Secretary-General, with the assistance of a group of governmental experts, to be established in 2009 on the basis of equitable geographical distribution, to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as the concepts referred to in paragraph 2 above, and to submit a report on the results of this study to the General Assembly at its sixty-fifth session;

5. *Decides* to include in the provisional agenda of its sixty-third session the item entitled "Developments in the field of information and telecommunications in the context of international security".

39 A/54/213, A/55/140 and Corr.1 and Add.1, A/56/164 and Add.1, A/57/166 and Add.1, A/58/373, A/59/116 and Add.1, A/60/95 and Add.1, and A/61/161 and Add.1.

40 A/60/202.

Developments in the field of information and telecommunications in the context of international security (Resolution 63/37 of 2 December 2008)

The General Assembly,

Recalling its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006 and 62/17 of 5 December 2007,

Recalling also its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community,

Recalling, in this connection, the approaches and principles outlined at the Information Society and Development Conference, held in Midrand, South Africa, from 13 to 15 May 1996,

Bearing in mind the results of the Ministerial Conference on Terrorism, held in Paris on 30 July 1996, and the recommendations that it made,[41]

Bearing in mind also the results of the World Summit on the Information Society, held in Geneva from 10 to 12 December 2003 (first phase) and in Tunis from 16 to 18 November 2005 (second phase),[42]

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Expressing its concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields,

Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

Noting the contribution of those Member States that have submitted their assessments on issues of information security to the Secretary-General pursuant to paragraphs 1 to 3 of resolutions 53/70, 54/49, 55/28, 56/19, 57/53, 58/32, 59/61, 60/45, 61/54 and 62/17,

Taking note of the reports of the Secretary-General containing those assessments,[43]

Welcoming the initiative taken by the Secretariat and the United Nations Institute for Disarmament Research in convening international meetings of experts in Geneva in August 1999 and April 2008 on developments in the field of information and telecommunications in the context of international security, as well as the results of those meetings,

Considering that the assessments of the Member States contained in the reports of the Secretary-General and the international meetings of experts have contributed to a better understanding of the substance of issues of international information security and related notions,

Bearing in mind that the Secretary-General, in fulfilment of resolution 58/32, established in 2004 a group of governmental experts, which, in accordance with its mandate, considered existing and potential threats in the sphere of information security and possible cooperative measures to address them and conducted a study on relevant international concepts aimed at strengthening the security of global information and telecommunications systems,

Taking note of the report of the Secretary-General on the Group of Governmental Experts on Devel-

41 See A/51/261, annex.
42 See A/C.2/59/3 and A/60/687.

43 A/54/213, A/55/140 and Corr.1 and Add.1, A/56/164 and Add.1, A/57/166 and Add.1, A/58/373, A/59/116 and Add.1, A/60/95 and Add.1, A/61/161 and Add.1 and A/62/98 and Add.1.

opments in the Field of Information and Telecommunications in the Context of International Security, prepared on the basis of the results of the Group's work,[44]

1. *Calls upon* Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field, consistent with the need to preserve the free flow of information;

2. *Considers* that the purpose of such measures could be served through the examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

3. *Invites* all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

   (a) General appreciation of the issues of information security;

   (b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

   (c) The content of the concepts mentioned in paragraph 2 above;

   (d) Possible measures that could be taken by the international community to strengthen information security at the global level;

4. *Requests* the Secretary-General, with the assistance of a group of governmental experts, to be established in 2009 on the basis of equitable geographical distribution, to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as the concepts referred to in paragraph 2 above, and to submit a report on the results of this study to the General Assembly at its sixty-fifth session;

5. *Decides* to include in the provisional agenda of its sixty-fourth session the item entitled "Developments in the field of information and telecommunications in the context of international security".

44 A/60/202.