ILLEGAL AND HARMFUL USE OF THE INTERNET

FIRST REPORT OF
THE WORKING GROUP

DEPARTMENT OF JUSTICE, EQUALITY AND LAW REFORM

BAILE ÁTHA CLIATH
ARNA FHOILSIÚ AG OIFIG AN tSOLÁTHAIR
Le ceannach díreach ón
OIFIG DHÍOLTA FOILSEACHÁN RIALTAIS,
TEACH SUN ALLIANCE, SRÁID THEACH LAIGHEAN, BAILE ÁTHA CLIATH 2,
nó tríd an bpost ó
FOILSEACHÁIN RIALTAIS, AN RANNÓG POST-TRÁCHTA,
4-5 BÓTHAR FHEARCHAIR, BAILE ÁTHA CLIATH 2.
(Teil: 01-6613111 – fo-líne 4040/4045; Fax: 01-4752760)
nó trí aon díoltóir leabhar.

DUBLIN
PUBLISHED BY THE STATIONERY OFFICE
To be purchased directly from the
GOVERNMENT PUBLICATIONS SALES OFFICE,
SUN ALLIANCE HOUSE, MOLESWORTH STREET, DUBLIN 2,
or by mail order from
GOVERNMENT PUBLICATIONS, POSTAL TRADE SECTION,
4-5 HARCOURT ROAD, DUBLIN 2.
(Tel: 01-6613111 – ext 4040/4045; Fax: 01-4752760)
or through any bookseller.

£5.00

PREAMBLE

In an age when accelerating change has become part of the very fabric of our society, there are few events or phenomena which are truly transformational in their nature. Even among such few transformations, however, it is difficult to conceive of any other development in modern times which comes near the transformational potential of the Internet. At the same time, it is also possibly the least understood of all modern developments and it is this very lack of understanding of its essential nature and its vast potential for society that sometimes impairs our ability to evaluate the many issues to which it gives rise.

While computer literacy is on the increase, the Internet still represents a vague concept to many people. Understandably, they find it difficult to grasp the idea of a network of networks of computers which has no central ownership, is almost indestructible and is growing at an unknowable rate. There is, however, nothing vague about its implications for the growth and well-being of Irish society and we must reach out and firmly grasp the full range of its commercial and educational benefits.

The Internet has been described as a mirror of society. Like a mirror, it reflects all aspects of life, good and bad. It reflects the outermost boundaries of human potential, limited only by our imagination. Sadly, such potential finds expression in both the positive and negative aspects of the human condition. It is this negative expression, regrettable though it may be, which is the focus for this Report.

In its mandate to examine the illegal and harmful use of the Internet, the Group was continually conscious of the need for balance in its treatment of the subject matter. The Internet allows the same ease of expression to evil as it does to good. In fact, it can be argued that with its relative anonymity and global dimensions, it facilitates the full expression of our darker side more than any other communication medium so far. To achieve an understanding of what we can do to address the downside of the Internet, we must first confront and understand the nature of the Internet. It is for this reasons that this Report discusses the background and the issues in some detail before recommending an appropriate response.

Without resorting to extreme, inappropriate and inevitably unworkable measures of censorship and restriction, the Internet will always include users who represent the darker elements of our society. The Group believes, therefore, that it is not a question of guaranteeing the removal of all illegal and harmful material on the Internet or of guaranteeing the impossibility of access to such material. Rather it is a question of working towards a safe environment for Internet users which will protect our children and respect the privacy and dignity of our citizens. Such an environment will, we believe, be created by practical national initiatives, intensive international co-operation and a heightened awareness and understanding of this phenomenon by all parts of society. Measures of this nature represent the backbone of the recommendations in this Report.

TERMS OF REFERENCE

To identify the nature and extent of the issues surrounding the illegal and harmful use of the Internet.

To prioritise such issues with particular reference to the need to address the issue of child pornography in the short term.

To examine and assess the current approaches both domestically and internationally to addressing the problem of the illegal and harmful use of the Internet.

In relation to those issues which can be domestically addressed, to identify the legal, technical and structural problems which arise and to make specific recommendations for their resolution in the short, medium and long term as appropriate.

In relation to those issues which require resolution in an international context, to make recommendations which will inform policy in this regard.

Téarmaí Tagartha

Chun nádúr agus fairsinge na nithe a bhaineann le mí-úsáid agus úsáid mhídhleathach an Idirlín a aithint.

Chun nithe dá réir a chur in ord tosaíochta i bhfianaise ach go háirithe an riachtanais chun deileáil le pornografaíoch leanaí sa ghearr-théarma.

Chun scrúdu agus measúnú a dhéanamh ar an gcur chuige atá ann i láthair na huaire, sa tír seo agus thar lear, d’fhonn tabhairt faoin bhfadhb a bhaineann le mí-úsáid agus úsáid mhídhleathach an Idirlín.

Maidir leis na nithe sin gur féidir tabhairt fúthu i gcomhthéacs na tíre seo, chun na fadhbanna dlíthiúla, teicniúla agus struchtúrtha a bhaineann leo a aithint agus chun moltaí sonracha a dhéanamh d’fhonn iad a réiteach sa ghearr-théarma, sa mheán-théarma agus san fhad-théarma, mar is cuí.

Maidir leis na nithe sin gur gá iad a réiteach i gcomhthéacs idirnáisiúnta, chun moltaí a dhéanamh a chabhróidh le cumadh polasaí ina leith.

TABLE OF CONTENTS

TABLE OF CONTENTS

APPENDICES PAGE

EXECUTIVE SUMMARY

BACKGROUND

➤ Internet not amenable to traditional analysis

The accelerated development of the Internet over the last few years is one of the most significant societal phenomena of the century and resonates through the commercial, economic, cultural, social and moral aspects of our lives. Any evaluation of this significance must, however, take into account the fact that as a phenomenon, it is in a state of constant and rapid evolution and our traditional tools of measurement and analysis do not readily lend themselves to forecasting its effects or planning our future responses.

➤ Need for balance

As with all such major developments in society, the Internet has its negative and positive influences. While this Report is mandated to evaluate its negative side, there is a constant need to strike the right balance between ensuring that we, as a country, are positioned to benefit from its many advantages and at the same time have a clear and structured approach to the protection issues which arise from its illegal and harmful use.

➤ New partnerships and approaches needed

These protection issues are wide-ranging, technically and legally complex and are international in their dimensions. They pose special challenges to the international community, governments, industry, educators, parents and indeed, individual users of the Internet. New partnerships, new approaches and new levels of flexibility will be needed to ensure that our exploitation of the Internet incorporates safety measures specifically designed to ensure maximum protection for those who are vulnerable to its downside.

➤ Child issues and framework strategy are a priority

The illegal and harmful use of the Internet involves a very wide range of issues including areas such as national security, child protection, economic security, racial discrimination, pornography, privacy protection, gambling, sale of controlled drugs, libel, and information security. Indeed, it can be said that almost all aspects of societal activity are part of an analysis of the downside of the Internet. However, in keeping with the priorities identified in its terms of reference, the Group focused for its first report on (a) an analysis of child protection issues and (b) the development of an overall framework within which these, and other downside issues, can be addressed.

➤ The Internet phenomenon

The analysis of Internet issues and the response to them is best understood against a backdrop of knowing its basic technology and the services which it provides. Essentially, the Internet is a “network of networks” of computers linked together using a series of protocols or rules which, for all practical purposes, represents a common language or Internet “Esperanto”.

The Internet can also be viewed as a source of services in the area of sound, text, and video. The main services include;

- the world wide web (WWW),
- electronic mail,
- discussion groups (newsgroups and mailing lists) and
- “Chat” (direct on-line communication).

Each of these services can be used in different ways to distribute and access illegal and harmful material and operate independently of where the material is accessed or stored. Each has different legal and policing implications.

THE "INTERNET FACTOR"

➤ **International phenomenon**
Because of the essential nature of the Internet, there are serious limits to what any one country can achieve on its own in the area of addressing the downside issues. The Internet itself is an international phenomenon in every sense of the word and any effective response will hinge on high levels of international co-operation.

➤ **Policing is difficult**
Tracing and proving illegal use of the Internet presents unique law enforcement challenges. Despite a proliferation of addressing systems, anonymous use of the Internet is still relatively easy and identifying the source of material placed on the Internet can be extremely difficult and indeed, sometimes impossible. The ease with which child pornography can be copied and disseminated in digital form is a serious barrier to any enforcement strategy which seeks to contain the problem.

➤ **Illegal use must be distinguished from harmful use**
Different approaches are required in relation to illegal and harmful use of the Internet. While the determination of illegal use is complicated, final decisions on legality in any given jurisdiction are determined by due legal process. Harmful use of the Internet is a much more subjective issue. What is considered harmful can vary between countries and indeed, within a particular country. It is sometimes a matter of taste, culture and value systems and is very much dependent on whether or not children are involved.

Response strategies will therefore vary in accordance with whether illegal or harmful material is involved Whereas responsibility for dealing with illegal material is ultimately a matter for the State, responsibility for screening harmful Internet material will increasingly devolve to the level of the individual.

Traditional forms of censorship will not operate effectively in the new borderless virtual environment of the Internet and individuals involved with children's use of the Internet, be they parents or educators, must share the responsibility of ensuring that a safe environment is provided. Software tools specially designed to screen harmful material are now becoming available which will facilitate such individual responsibility.

➤ **Phenomenal pace of change**
The responses to the challenges posed by the illegal and harmful use of the Internet must be sufficiently flexible to reflect rapid changes in Internet technology and services. Measures which do not provide for review and adaptation are not suited to an environment characterised by constant evolution. The specific measures suggested in this Report must be seen in the context of the particular stage reached in Internet development and must be sufficiently flexible to accommodate change.

THE ISSUES

➤ **Child protection**
The range and quality of services offered by the Internet makes its use very attractive for paedophiles. Quantification of the extent of the problem is difficult due to factors already mentioned but there are clear child protection issues involved. Research available to the Group, in particular the study by Professor Max Taylor from UCC, indicates that the Internet continues to be a major (if not the major) focal point for the distribution of child pornography and information about paedophile behaviour. No more than in other countries, the child protection issue is a serious one and must be addressed.

➢ Legal implications

The Internet operates on an international basis. The law operates on a territorial basis. Thus we have the genesis of many of the legal issues surrounding the Internet. Material on the Internet is held worldwide and can be accessed worldwide. Some material is held and accessed locally. Other material is held outside the jurisdiction and is only accessed locally. The extent to which national law operates can therefore be a complex issue to decide. Liability issues often turn on the extent to which any particular party controls, or is aware of, illegal content. The concept of being aware or "knowing" has its own difficulties arising from the way in which the underlying Internet technology works.

➢ Blocking illegal content

The very nature of the Internet poses limitations on the ability of service providers to block specified material particularly when there is no absolute way of knowing the full nature of the material, even if it is held within the jurisdiction. Blocking access to foreign web sites represents a particularly difficult problem.

It is important to understand that the issue is not about guaranteeing the blockage of all harmful and illegal material. It is more about adopting feasible policies in this area which;

- are sufficiently discriminatory and effective so as to maximise the full benefits of the Internet,
- are in conformity with legal provisions, and
- respect, in particular, the protection and interests of children.

This difficult task is best fulfiled in the context of a constructive partnership of all parties and an appropriate forum for common decisions on the many sensitive issues involved. The establishment of such a forum is among the recommendations in the Report.

➢ Need for new structures

While there is a need to ensure that any new arrangement will attract the co-operation of all parties, the Group does not favour the introduction of statutory structures. We believe it is not only impossible but also counter-productive to attempt to "regulate" the Internet in the sense of introducing new national statutory provisions to specifically control its illegal and harmful use. The defining characteristics of the Internet already mentioned and explored in detail in the Report, do, we feel, reflect that belief. This is not to say that our national laws should not continue to take careful cognisance of the emerging technology; "Internet proofing" of new legislation is among our recommendations.

The downside of the Internet, irrespective of the different perspectives and interests involved, represents a common enemy which will only be defeated through partnership and co-operation. This new partnership approach will involve new structures and active participation by all parties, but with the service providers having a key role. The positive co-operation shown so far by the Internet Service Provider's Association of Ireland (ISPAI) is an indication of how much can be achieved in a partnership arrangement.

A partnership approach, characterised by a willingness to see all issues as common problems and supported by Government and the service provider industry, is the best way forward at this point in time.

➢ Awareness

A realistic assessment and knowledge of the issues involved in this complex area is essential for an appropriate and workable response to the downside issues. Moral panic based on poor understanding of the Internet is an enemy to progress. Awareness is a key part of any overall national strategy in this area and the Report makes detailed recommendations in this regard.

INTERNATIONAL EXPERIENCE

A detailed analysis of international experience was carried out by the Group and is shown in Part 4 of the Report. There has been an acceleration of international studies of the downside of the internet over the first year with the realisation that very high levels of international co-operation will be needed to successfully address the issues. Initiatives are emanating from several areas within the EU and considerable effort is being put into co-ordinating the various responses. The OECD is also involved in a significant study of Internet content issues and US experience is also of great interest and relevance.

In essence, at least within the European context, international developments are broadly in line with the strategy envisaged in the Report. A self-regulation approach by service providers linked with new structures which include hotlines and overarching supervisory groups, are either already established or being contemplated by most EU member states. Voluntary codes of practice rather than strong regulatory mechanisms predominate, and while specific national initiatives are important, there is a growing realisation that no one country can make effective progress in isolation.

PROPOSED NATIONAL STRATEGY

➤ Criteria

The Group's criteria for establishing a new strategy was that it should:

- reflect practical measures which can be implemented in the short term
- be capable of directly addressing the issue of child pornography
- be compatible with the overall national objective of extracting maximum economic and social benefit from the Internet
- be geared to the particular economic, legal and social conditions in Ireland
- be capable of being integrated with ongoing international developments

➤ Strategic components

The package of strategic measures focused on four main areas:

- the introduction of a system of self-regulation by the Internet service provider industry to include common codes of practice (COPs) and common acceptable usage conditions (AUCs)
- the establishment of a complaints hotline to investigate and process complaints about illegal material on the Internet
- the establishment of an Advisory Body on the Internet to co-ordinate measures so as to ensure a safe Internet environment within the self-regulatory framework
- the development of awareness programmes for users which will empower them to protect themselves, or others in their care, from the illegal and harmful material on the Internet

➤ Self-regulation

This is a key building block in a national strategy for addressing the downside of the Internet and should be pursued as a matter of priority. Self-regulation by the service providers should include the development of codes of practice focusing on:

- promoting a general awareness of safety issues on the Internet
- establishing a common approach as to how content filtering facilities can be made available to individual users
- defining procedures for interacting with other players in the self- regulating environment
- establishing procedures for ensuring compliance

➤ Establishment of the hotline

The main functions of the hotline would be as follows:

- investigation of complaints about illegal material on the Internet
- taking action as a result of the investigations
- promotion and assistance in developing rating systems for Irish-based Internet material
- co-operation with international hotlines
- public reporting on its activities
- reporting to the Advisory Board on the Internet

As a matter of principle, funding of the hotline should be provided by the service provider industry. However, because of market size and stage of development, the industry is not in a position to provide the funding which will be needed immediately to establish the hotline. Funding support should therefore be provided by Government at least in the short term pending the establishment and consolidation of the industry on a more substantial footing. Discussion should take place with the industry on detailed funding arrangements.

➤ Establishment of Advisory Board on the Internet

The hotline will need advice and assistance from a partnership-driven forum which will itself monitor and promote the overall self-regulation framework. Members of the Board will include service providers, the Gardaí, Internet users, Government, the Information Society Commission, education and child protection bodies, a legal advisor and the Director of the hotline.

The Board's functions will include:

- setting up the hotline and its working procedures
- promotion of self-regulation measures to ensure a safe Internet environment
- contribution to the development of standards
- making decisions on issues arising from hotline activity
- international liaison
- carrying out a regular review of the appropriateness of new structures
- reporting to Government and Industry on progress

In view of the critical and immediate role to be undertaken by the Advisory Board on the Internet, it is recommended that the Secretariat be supplied by Government and that funding be provided to enable it to carry out its designated functions.

➤ Awareness measures

The development of appropriate awareness measures is a critical complementary tool in addressing the illegal and harmful use of the Internet. Specific measures should include:

- integration with awareness initiatives already recommended by the Information Society Commission
- awareness measures by all constituents of the new structures, e.g. service providers, hotline, advisory board etc.
- specific sectoral awareness initiatives, particularly in the schools area

WORKING GROUP'S NEXT STEPS

The terms of reference given to the Group in 1997 were broad enough to allow it to continue examining other issues relating to the illegal and harmful use of the Internet. As already pointed out, however, we are working in a rapidly evolving environment and we ourselves must adjust our work focus to new national and international developments. Against this background, the first task of the Group will be to re-examine its composition and prepare a new set of priority issues for our next Report.

SUMMARY OF MAIN RECOMMENDATIONS

Self-regulation

A system of self-regulation by the service provider industry should be introduced to include common codes of practice and common acceptable usage conditions. (5.1.3., 5.2).

Complaints hotline

A non-statutory national complaints hotline should be established to investigate and process complaints about illegal material on the Internet. (5.3)

Advisory Board

A non-statutory Advisory Board representative of the significant players involved should be established to oversee and co-ordinate measures aimed at ensuring the success of the self-regulatory framework. (5.4)

Awareness

Any national awareness campaigns proposed by the Information Society Commission should include a dimension which addresses the potential for illegal and harmful use of the Internet. (5.6)

Other awareness measures should include: (5.6.3)

- An active role for service providers in the education of their clients on the safe use of the Internet.
- The active involvement of the new hotline and Advisory Group in the development of awareness programmes.
- The specific targeting of parents and teachers
- The incorporation of modules on Internet safety into the curriculum of teachers, care workers, Gardaí, Customs officers and any other agencies who come in contact with issues relating to the downside of the Internet.

Specific initiatives for schools should include: (5.6.3)

- In-career training modules for teachers on Internet issues
- The publication of a set of guidelines by the Department of Education and Science for those involved in the Internet in schools.
- The integration of Internet Ethics into the Curriculum
- The staging of information sessions for Parents/Guardians.
- The development of a Schools Code of Conduct

Funding

The initial funding of the hotline should be shared by Government and the service provider industry (5.7.4.)

In view of the critical and immediate role to be played by the Advisory Board, its Secretariat should be provided by Government. (5.7.5)

The service provider industry should immediately and actively pursue EU funding opportunities which are now available in the area of Internet safety. (5.7.6)

Legislation

New legislation and any reviews of existing legislation should be “Internet proofed” before being submitted to Government for approval. (5.8.1.)

Specialist training

Specialist training programmes already begun in the Garda area should be urgently pursued and extended to the wider areas of law - enforcement including the judiciary. (5.8.3)

Introduction

1

INTRODUCTION 1

1.1 ESTABLISHMENT OF GROUP

In response to the Taoiseach's request to the Minister for Justice to establish a Working Group on the illegal and harmful use of the Internet, draft Terms of Reference and proposals for membership were submitted to Government in mid-February, 1997. The inaugural meeting of the Group took place on 25 February and the deliberations of the Group extended over a period of 11 months. A total of 13 plenary sessions were held. Each of four sub-groups also had several meetings in the context of discussing particular topics. A full membership list is given in Appendix 1.

1.2 METHODOLOGY

The Group was conscious from the beginning of the enormous range of issues encompassed by the Terms of Reference. In keeping with the priorities relating to child pornography and because of the need to establish a framework within which progress could be quickly made, a work programme was established geared to tackling the issues capable of being addressed in the shorter term. Sub-groups were formed to carry out a detailed assessment of four major areas as follows:

A total of 47 written submissions were received

- Legal implications.
- International aspects.
- Child issues.
- Issues relating to the role of Internet Service Providers (ISPs).

Separate chairpersons were appointed by each group and individual group reports were drafted, discussed and ultimately agreed by the plenary group.

As part of the initial assessment of the issues, the plenary group attended a technical demonstration of the Internet which included an examination of child pornography material. This examination was based on research carried out by Professor Max Taylor, University College Cork, who is a member of the Group.

Invitations for submissions to the Working Group were publicly advertised in August, 1997 and a total of 47 written submission were received either by letter or by e-mail. The Group also heard a further 6 detailed oral presentations. Based on their particular experience in the area of combating child pornography on the Internet, David Kerr of Internet Watch Foundation (UK) and Nigel Williams of Childnet International were also invited to address the Group. A full list of submissions is shown in Appendix 2.

A further 6 detailed oral presentations were heard

1.3 FOCUS OF GROUP

As already stated, in view of the breadth and complexity of the subject under review, and the need to concentrate on taking practical steps in the short term, the Group carried out a preliminary examination of the range of possible issues involved in the illegal and harmful use of the Internet.

1.3.1 Illegal uses

While the concept of illegal use is very much associated with child pornography, the terms cover a very wide range of issues. Illegal uses may be described under a number of headings:

National security:
- Terrorist activities
- Instructions on bomb making
- Hacking into government computer networks

Injury to children
- Child pornography
- Adult pornography
- Material depicting extreme violence
- Child trafficking
- Advice on anonymous exchange of graphic material

Injury to human dignity
- Racial discrimination, incitement to racial hatred
- Extreme sexual perversion

Economic security
- All types of fraud
- Instructions on credit card piracy

Information security
- Malicious hacking

Privacy protection
- Unauthorised mailing
- Interception of personal e-mail
- Misuse of personal data
- Unfair obtaining of personal data

Protection of reputation
- Libel

Gambling

Information on or sale of “controlled drugs”

Intellectual property
- Copyright infringements of any medium
- Unauthorised distribution of videos, music, software etc.

1.3.2 Harmful uses

Harmful uses are difficult to identify as they involve an assessment of effects on individuals

The European Commission’s Green Paper[1] refers to using the Internet as a medium to communicate information which, while not illegal per se, might nonetheless have the capacity to affect the physical or mental development of vulnerable individuals, particularly minors. This could be interpreted as a possible definition of the harmful use of the Internet. The Group feels, however, that harmful uses are difficult to identify with any great precision since they involve an assessment of their effect on different individuals. This could include material relating to sex, violence, discrimination, graphic crime reporting, drug addiction, and cult worship. While not explicitly prohibited by law, this kind of material could, in the context of certain individuals, result in harm.

1.3.3 Final emphasis

Having briefly considered this wide range of issues, the Group decided, in keeping with its terms of reference, to concentrate on measures which would (a) address the protection of children (b) yield results in the short term and (c) provide a framework within which progress could be achieved. This Interim Report therefore addresses:

- the specific question of child pornography;
- the more general question of structures which would be needed to underpin initiatives in this area.
- legislative implications; and
- international aspects.

These topics reflect the work of the sub-groups already described.

[1] Green Paper on the Protection of Minors and Human Dignity in Audio-visual and Information Services. European Commission document (96) 483, 16 October 1996

1.4 A MOVING TARGET

As the work of the Group progressed, a number of significant developments, difficult to anticipate, shaped the focus and emphasis of our work. Indeed, given the phenomenal pace of developments in the Internet area, the scenario being reported on at the time of writing this Report is quite different from that which the Group faced in March, 1997. There is little doubt that this extraordinary rate of change will continue into the future.

The extraordinary rate of change will continue

1.4.1 Need to consider Child Pornography Bill

A consideration of the emerging legislation on child pornography became crucial to our deliberations as it had significant implications for the issues being considered by many of the sub-groups. While it is appreciated that the Child Trafficking and Pornography Bill 1997 had a wider focus than the Internet and is drafted in general terms, many of its provisions had a direct bearing on the final composition of our recommendations, particularly in the structural area. The Group is grateful for the co-operation extended to it by the Law Division of the Department of Justice, Equality and Law Reform in listening to the views of the Group and for reflecting some of these concerns in the final shape of the Bill.

1.4.2 Emergence of ISPAI

At the time of the inaugural meeting of the Group, the contributions from the service providers was, for pragmatic reasons, generously supplied by Mr. Colm Grealy from Ireland-On-Line. As the deliberations of the Group continued, however, the need for an umbrella association, independent of any particular provider, became increasingly important. With enormous co-operation from the main Irish service providers and with the encouragement of the Working Group, the Internet Service Providers Association of Ireland (ISPAI) was formed in April 1997 with Mr Cormac Callanan as its first Chairperson. Membership of the ISPAI is shown in Appendix 3.

The Group spent some time assisting in the development of discussion material for the new Association in order to bring it up to date with the issues under consideration. It must be said that the contribution of the Association has been crucial to the work of the Group. Its continued development and the degree to which it represents the interests and combined energy and resources of all providers, will be a crucial aspect of success in implementing many of our recommendations. It should be noted that the composition and ownership of the Service Provider Organisations themselves went through significant change during the lifetime of the Group; this will doubtless continue to evolve as the Internet market develops in Ireland.

ISPAI involvement will be crucial to success

1.4.3 International developments

The third significant development which took place contemporaneously with the deliberations of the Group, related to the international scene and this is described in detail in Part 4 of the Report. In October 1996 the European Commission approved a Communication on Harmful and Illegal Content on the Internet and a Green Paper on the Protection of Minors and Human Dignity in the context of Audio-visual and Information Services. The two documents, which are complementary, were proposed at the initiative of Martin Bangemann, Commissioner in charge of Information Technologies and Telecommunications and Marcelino Oreja, Commissioner in charge of Cultural and Audio-visual Affairs.

In November 1997 the European Commission approved a Communication as follow-up to the Green Paper which included a proposal for a Council Recommendation concerning the protection of minors and human dignity in audio-visual and information services. The proposal is currently being examined by the Council Audio-visual Working Group and it is the intention of the UK Presidency of the Council that the Recommendation will be adopted by the Audiovisual/Culture Council in May 1998.

As recently as January 1998, an Action Plan focusing on funding proposals for specific projects aimed at a range of measures for ensuring the safe use of the Internet, was put forward by the European Commission.

In summary, the Group found itself dealing with a range of important unfolding developments and is conscious that its Report must be considered in the context of a continually evolving situation. The recommendations of the Group are, however, geared as far as possible to such an evolving environment and are focused on the structures within which such evolution can be harnessed to address the emerging issues.

1.5 ILLEGAL VERSUS HARMFUL MATERIAL

In order to complete an understanding of the Group's overall approach, the separate concepts of "illegal" and "harmful" need elaboration.

1.5.1 The concept of Illegal

What is illegal off-line is illegal on-line

What is illegal varies from jurisdiction to jurisdiction and illegality is determined ultimately by the Courts in that jurisdiction. It is not a question of taste, individual judgement, culture or the age and background of those affected by the material. The process of determining illegality is quite structured and involves reporting, assessing, evidence gathering, prosecution and trial and in the event of a criminal conviction, eventual sentencing. While there may be some implications for the way in which we frame our national law, illegality arises irrespective of the medium used. The Internet does not create a legal vacuum. To use the international phrase which has become a by-word in this context; "*what is illegal off-line is illegal on-line*".

It must also be remembered that the mere fact that the Internet is a new phenomenon does not automatically render inapplicable all existing laws. Simply because a particular piece of legislation was enacted at a time when a particular type of technology was not in existence does not automatically mean that the technology is not covered by that legislation. As referred to later in this Report, the Video Recordings Act, 1989, for example, does not refer specifically to the Internet. However, it may be applicable to the supply of certain types of video over the Internet.

One further complication must now be introduced. The Internet is, by its nature, international. Material on the Internet is held throughout the world. Access is made to that material from all parts of the world. One country cannot control material held in another country. In many cases there are even serious limitations on the ability of a country to control access by its citizens to both foreign-held and locally-held material.

We do not, therefore, have a neat, controllable situation where the traditional application of national law will apply. While the problem of national legal jurisdiction is, at best, a sensitive and complex area, the Internet, by its very nature, poses even greater challenges in this regard.

There are, however, obvious occasions where illegal material on the Internet will, in fact, come within the jurisdiction of a particular country. In such cases, national law will apply and the appropriate structural and legal framework must be in place. It is easy to see that intensive international co-operation will be crucial in ensuring that the national laws of different countries can be brought to bear on illegal Internet material, depending on where such material is held.

Illegality in one country may not be illegality in another

This approach is, of course, mediated by the reality that different countries have different national laws. What is illegal in one country may not be illegal in another. Within the European Union, the ongoing process of legal harmonisation will help, but as already pointed out, we are dealing with a global phenomenon where the laws of every country in the world are relevant to the issue. International co-operation is, therefore, a fundamental prerequisite for addressing illegal use of the Internet.

1.5.2 The concept of harmful

The question of harmful use of the Internet is quite different in that it raises different issues and requires a different approach to its resolution. As mentioned in Paragraph 1.3.2., meaningful definitions of “harmful” are difficult to compose, and the focus is on material which, while not illegal, is capable of causing harm to the individual. This harm can arise because of particular characteristics of the individual, age, sex, race, etc. or it can be linked to the nature of the material itself. For example, the material could be degrading in itself, be composed of lurid sexual content, or induce children to spend foolishly.

Harmful use raises different issues and needs a different approach

There is little new in society taking the view that vulnerable people should be shielded from material which could harm them. We already have a long tradition of rating systems for videos and films, watershed hours for television broadcasts and age restrictions for particular functions and events. Illegal material is usually, by its nature, harmful. Society has, in these cases, decided to pass laws to address that harm. Whereas the State makes controlling decisions on such material through its laws, the control of harmful material which is not illegal must lie more in the domain of the individual.

Decisions on acceptability of harmful material are subjective and are very much context-based. There are variations in levels of acceptability not only between countries but also within countries. What some people might find distasteful and offensive, others may not. While the cultural norms may mediate what is considered to be “acceptable”, any form of consensus is, at best, problematic. What is required in this area is not the harmonisation of laws but rather the opportunity for individuals to make an informed decision about harmful material on the Internet on behalf of themselves and those under their care. The solutions and general approaches to harmful use of the Internet are therefore quite distinct from those relating to illegal use. Fortunately, the tools to facilitate such individual decisions are becoming available and will be discussed later in the Report.

2

What is the Internet ?

WHAT IS THE INTERNET? 2

A basic understanding of the technology is essential

Before discussing issues or indeed putting forward responses to those issues, it is essential to have a basic understanding of what constitutes the Internet. It is beyond the scope of this Report to provide a comprehensive description of the Internet in technical terms but the following paragraphs seek to outline the main ingredients relevant to the material in the Report. A glossary of common Internet terms is given in Appendix 4.

To those whose contact with the Internet is confined to the popular media, it may appear to be a confused amalgam of abbreviations, acronyms and technical terms. Many of these terms are rapidly becoming part of our everyday language. References to the Web, Home Pages, and e-mail addresses abound as the Internet phenomenon forces its way into our daily lives.

2.1 THE PHYSICAL BACKBONE

At a physical level, the Internet is a vast system of connected computers. A particular set of connected computers is called a “network”. To conceive of the “Internet”, one must go somewhat further than a single network of computers. We must think in terms of a “network of networks” of computers. Thus, we have the term “inter” “net” - networks communicating between themselves. The computers on this “network of networks” have a very important capability - they speak the same language - a form of Esperanto of the electronic world. Many of the special terms and abbreviations relate to the different languages, protocols or rules used in this universal communication process. Effectively, the Internet is able to operate as if it was a single network speaking the same language even though it contains many different networks of computers ranging from small local networks to large international ones.

New developments are constantly emerging. “Intranets” use Internet technology to allow business to create its own internal networks. “Extranets” use Internet technology to allow communication with a chosen subset of a particular business community.

2.2 THE SERVICES

Understanding the differences between the services is also crucial

Even though the above represents the physical backbone to the Internet, it is perhaps best conceived of as a source of services and communication tools. It should be noted that the services involved are multi-media (i.e. they provide for text, audio, video, graphics etc.). The main services include:

- the World Wide Web (WWW)
- Electronic Mail (e-mail)
- Discussion groups (newsgroups and mailing lists)
- Chat

From the perspective of pinpointing the illegal and harmful use of the Internet, it is important to understand that these services operate in very different ways. Tracing the source and use of such services by individual users can range from relative ease to near impossibility. In some cases, the issue revolves around access to the services while in other, the issue involves the location of where material is created or stored. Since such distinctions are crucial, each service will briefly be examined.

2.2.1 The World Wide Web (WWW)

The WWW represents a vast library of documents, referred to as “Web Pages” which, even though physically scattered throughout the networks of the Internet, can, from a user point of view, be accessed and viewed as if they were in a single library system. Information, (text, video, audio etc.) placed in this library is immediately accessible by all Internet users. Behind the WWW is a very powerful set of tools. For example, in much the same way as a video player is needed to play a video, a web “browser” is required to browse or examine the contents of the WWW. Browsers are becoming more and more sophisticated and their functions are continually expanding.

WWW material can be stored anywhere and be accessed from anywhere

Having such a vast library of “pages”, or documents is of little advantage if the information cannot be easily retrieved. The indexing of the information is done through what are called “search engines”. These allow the user to type in a specific topic and to be guided through all the references in the WWW known to the search engine on that particular topic.

Moving from one page to the next is done by the user clicking a mouse on specially coded “links” built into each page and readily identifiable to the user. Such links, when activated by the user, can switch to any other part of the entire contents of the Internet. Clicking on a link in Dublin can automatically access a page which has been created and stored on the WWW, say, in Australia. The people who created that page in Australia would not necessarily be aware that their page was being linked to, nor would their permission necessarily be required.

It can be seen, therefore, that material held on the WWW can be stored anywhere throughout the world and be accessed from anywhere around the world. In terms of illegal or harmful material existing on the Web, issues emerging include: access to Web pages by children; the location of the computer where the pages are physically stored (and thus the jurisdiction within which such material will be assessed); and the tracing of the persons who were responsible for authoring Web pages.

2.2.2 Electronic Mail

E-mail can be used for illegal purposes

Despite the perceived popularity of the WWW, e-mail is still the Internet’s most used feature. As the name suggests, it enables mail to be sent between users of the Internet. The particular software tools and protocols behind e-mail make a very simple task of the whole process of using the Internet mail system. As with the traditional postal system, the only requirement is to know the Internet address of the other party. At any one time, therefore, there are millions of mail messages circulating around the Internet following unknowable physical paths, sometimes being split into discrete parts en route but yet being re-assembled successfully at their final destination at the address quoted by the sender. As with the WWW, the messages are not confined to text but can include visual and audio attachments.

From the perspective of the potential to misuse the Internet, it can be seen that e-mail represents a service which has much to offer those who would wish to communicate on illegal matters or who seek to send or swap illegal graphical material without drawing the attention of the law enforcement authorities. The presence of such material on the Internet can be transient. Once a message is sent and received, any trace of it can disappear completely from the computer networks of the Internet.

2.2.3 Discussion groups

Newsgroups

This term is somewhat misleading as it does not refer to the traditional use of the term “news”. These are public discussion fora on every imaginable topic which are organised into discussion topics called newsgroups. Newsgroups have their own indexing system and are organised hierarchically by subject matter. Users can read and reply to “articles” in the newsgroups.

Individual service providers in individual countries “subscribe” to particular newsgroups so that the newsgroups available to particular users are determined by choices made by the service provider. As with all the Internet services, powerful tools allow the user a simple to way to access and contribute to newsgroups. There are tens of thousands of newsgroups in many different languages on the Internet and they are stored on separate computers called news servers. Because of the enormous amount of newsgroups, not all newsgroups are available on all news servers.

Newsgroup availability is generally determined by service providers

Again, it is useful to note that from the perspective of the misuse of these newsgroups, access to them works on a different principle than, say, the WWW. The choice of newsgroups on offer to a particular user sometimes arises from commercial and technical decisions by service providers. The particular choice of newsgroups can also arises from a decision not to offer particular newsgroups which suggest an obvious illegal/harmful content. Some newsgroups can, simply by observing their name, be considered to be unacceptable for delivery to users. Examples would include alt.sex.bestiality and alt.sex.paedophile.

It should be noted also that while service providers store newsgroups locally, it is possible for Internet users to use the service providers merely as a conduit in getting access to newsgroups held outside the jurisdiction. This, of course, complicates the whole question of newsgroup access from the point of view of their illegal and harmful use.

Mailing Lists

The main difference between newsgroups and mailing lists are in the way in which they are distributed. As stated, newsgroups are distributed through a special USENET system, whereas mailing lists are distributed by simple e-mail. Contributions are made to a particular e-mail address and this acts as a post box for distribution to a predefined list of addresses. Users on the address list get copies of all the mail. These lists can be public or by invitation only, thus complicating the problem of detecting their misuse.

2.2.4 Chat

This service allows users to talk to each other in real time, i.e., as a message is typed by any one user, it is seen immediately by all those who are “logged” into that particular chat session. The Internet’s largest chat system is called IRC (Internet Relay Chat). As with all the other services, IRC is supported by tools which allow users of the Internet to browse channel topics which may be of interest to them. Chatting on-line is somewhat like CB radio - a user tunes into the channel by logging in. Any user of the channel can see the names of other contributors, although nicknames are commonly used. While representing a powerful facility to those who would wish to converse in this manner, the scope for harmful and illegal use is obviously immense and is often used for paedophile purposes. It is also possible to have closed discussion groups by prior arrangement - thus contributing to the scope for illegal use.

It is also possible to have closed discussion groups

2.3 ADDRESSES ON THE INTERNET

Underlying all these services is a comprehensive system of Internet addressing which is used to identify users, computers and various other constituents such as files, Web pages etc. that make up the Internet. For example, someone using e-mail has a special e-mail address which has a particular format used by the appropriate software. A typical mailing address would look like jbloggs@irlgov.ie

Every computer while connected to the Internet has a unique four part number called an “IP address” and would appear like 32.102.45.26. However, to help users in finding particular computers, most computers connected to the Internet have a “domain name” written in a more meaningful, language-based way to correspond to its IP address. A basic domain name (sub domains are also possible) would appear like www.irlgov.ie. Documents and files available on the WWW have a unique address called a URL (Universal Resource Locator). These are the kinds of addresses which are usually advertised in magazines and television. They enable the user to make direct contact with that particular Web site. They have the form http://www.irlgov.ie/justice/default.htm

Anonymous use is still possible despite addressing systems

While it might be expected that the presence of such specific addresses would allow all activity on the Internet to be traced and monitored if one so wished, this is not the case. The anonymity which can be associated with the use of the Internet has serious implications for examining its illegal and harmful use and poses special problems for law enforcement agencies. Specific services are available to disguise e-mail addresses. Web sites can be moved to new locations. Illegal or harmful newsgroups can be re-created under new names or can be accessed through international rather than national news servers. In addition to all this, cheap effective encryption can be used to ensure that even if illegal material is suspected, it cannot be deciphered.

2.4 THE PEOPLE INVOLVED

The final piece in this Internet jigsaw relates to the players. With today's level of development of the Internet, there are a host of specialisms emerging and these are still in the process of evolution. Some of the players are inter-changeable and perform multiple roles. Users of the Internet can also be the suppliers of content. Business and Government are both users and suppliers. Added-value on the Internet in all its forms is itself becoming a growth industry and the distinctions between traditional professions are becoming blurred. For example, "Publication on the Internet" is one of the new growth industries.

Distinctions between traditional professions are becoming blurred

In terms of a discussion of the issues relating to illegal and harmful use, each player is positioned differently in terms of (a) how much they control the use and content of the Internet; (b) their liability arising from such control; and (c) the effectiveness of their role in combating illegal and harmful use.

2.4.1 Significant players

For the purposes of this Report, however, a number of distinct groups can be identified. These include:

- Users
  Those who use the various services of the Internet - individuals, schools, business, Government etc.

- Content providers
  Those who specialise in providing information on the Internet. Providers can obviously be domestic or international - the Internet makes no distinction.

- Service providers
  Those who provide easy-to-use connections to the Internet and access to all Internet services. In the early days of the Internet, connection required a high degree of technical expertise. Over the years and with the emergence of improved software tools and the developing role of the service provider, connection to, and use of, the Internet requires little technical knowledge and meaningful use by the novice user can be obtained from the Internet after a few minutes. It is not, however, a simple question of the service providers' role being confined to making the physical connection to the Internet. Service providers have a wider range of functions which support users in interacting with the Internet.

Service providers have a pivotal role in tackling downside issues

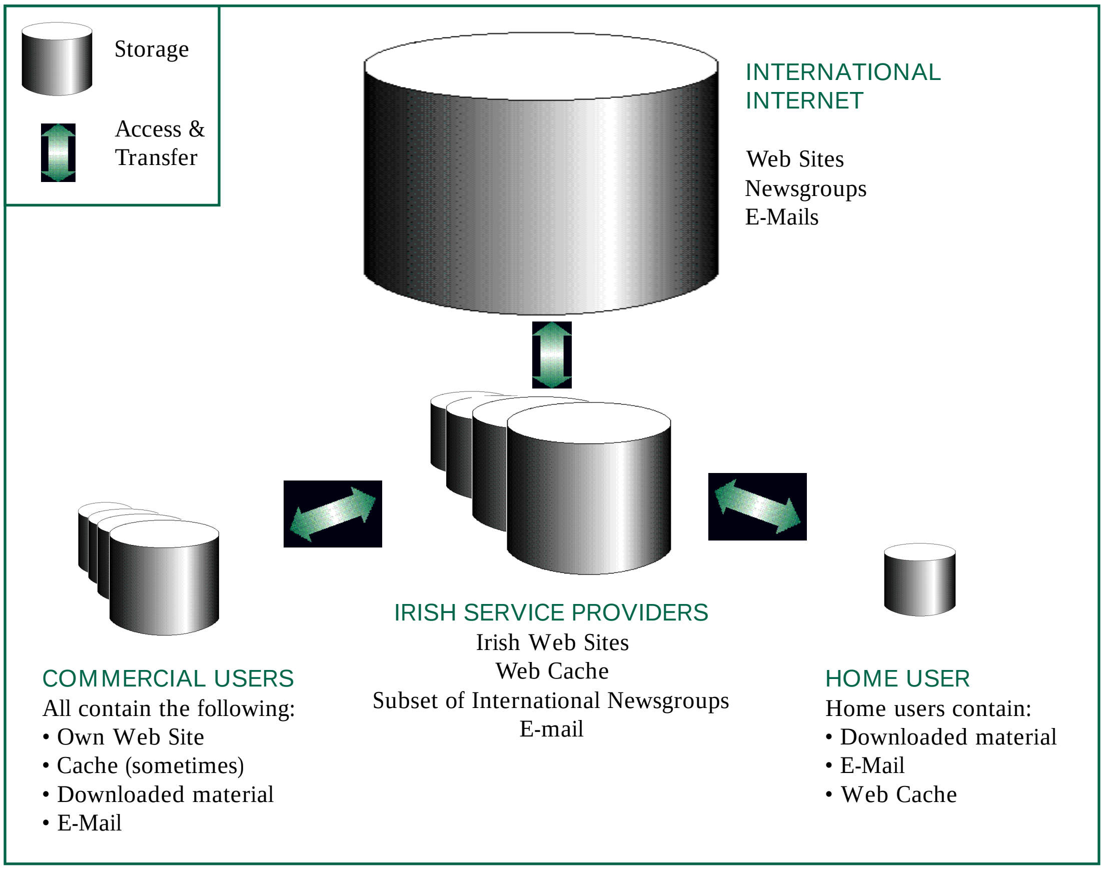
When a user decides to opt for a particular service provider, he or she is given a package of tools which provide an easy-to-use interface with a whole range of services. These services include browsing the WWW and sending and receiving e-mail messages. In essence, service providers provide the interface between the Internet and its users. Their range of added-value services continues to develop and expand and the rapid changes in the ownership and structure of the Internet service provider market in Ireland continues to reflect that expanding role in an increasingly competitive environment. It is because of their pivotal role in interfacing between the user and the Internet that service providers are central figures in addressing issues arising from the illegal and harmful use of the Internet.

- Telecommunications network providers
  These organisations provide the backbone network services on which the Internet runs. While appropriate technical regulation is essential in this area, these organisations have little role in the area of content control.

- Broadcasters
  Those who provide services using technology such as satellite, cable and television signals and provide Internet services directly to the home, bypassing local Internet service providers.

2.5 STORING AND ACCESSING INTERNET MATERIAL

The simplified diagram below illustrates in very broad outline how information is held and accessed on the Internet.



3

The Issues

THE ISSUES 3

3.1 PROTECTING CHILDREN

3.1.1 Disappearance of traditional control mechanisms

One of the primary issues addressed by the Group in the context of the illegal and harmful use of the Internet related to the protection of children. It is clear from the discussions so far that the Internet is poised to significantly affect all aspects of our lives. Developments in travel over the last few decades have led to the view that the world is getting smaller - we live in the so-called "global village". In another sense, it can be argued that at least from the individual's point of view, the world is, in fact, getting bigger as the Internet opens up an expanding resource of information from all around the globe.

Opinions, events, analyses, art, entertainment, news, and unfortunately a large measure of illegal and harmful material, are all available at the click of a mouse, irrespective of where they originate. National cultures, for so long bounded and protected by physical boundaries may survive, or as the case may be, fail to survive, in the unprotected virtual environment of the Internet. To the extent that national cultures and norms were mediated by censorship mechanisms which relied on the physical transportation and distribution of material such as films, videos, magazines etc., those protections have gradually given way to the borderless virtual world of electronic networks.

We need to protect our children

The challenges represented by these new forces are great. The potential for benefiting society is also great. As a maturing society, we can grow and come to terms with these broader horizons. However, the greatest challenge facing us is not, perhaps, our ability to reap the full benefits of the Internet but rather to ensure that in the process, we protect that section of our society whose maturity and ability to deal with a changing world needs nurturing in a safe environment. We need to protect our children.

3.1.2 Effects of the Internet on children

The Internet, as a global information medium, is likely to affect children in several ways. Some examples in this areas were indicated by Children Now, an American organisation who identified a number of key areas as follows:

- Education
  Access to the information super-highways in the classroom is likely to have a major impact on the content and the quality of education, creating possibilities to either address or significantly worsen educational inequities.

- Home Entertainment
  Greater levels of access to Internet content, whether informational, educational, violent, pornographic or otherwise harmful, will accelerate the need for practical control mechanisms.

- Quality of Life
  Children may soon spend more time interacting with others through their television sets or computers, than interacting with one another, taking physical exercise or reading.

- Provision of Services
  The Information Super Highways make it possible to deliver a multitude of services directly to children and their families, including financial assistance and health care. There is also an opportunity for children to perpetrate fraud, through, for example, accessing services using false credit card details.

3.1.3 Effects of harmful Internet material on children

Important distinctions between the concepts of “illegal” and “harmful” have already been made in the introduction to this Report. It has also been pointed out that, in general, illegal material usually tends to be harmful. However, much Internet material, although it may not be illegal, can have harmful effects on a child.

The European Commission Green Paper[2] draws a distinction between material which is illegal and unsuitable for viewing irrespective of the viewer's age, and that which is undesirable for children:

> *It is important to distinguish two types of problem relating to material:*
>
> *Firstly, access to certain types of material may be banned for everyone, regardless of the age of the potential audience or the medium used. Here it is possible, irrespective of the differences in national legislation, to identify a category of material that violates human dignity, primarily consisting of child pornography, extreme gratuitous violence and incitement to racial or other hatred, discrimination and violence.*
>
> *Secondly, access to certain material that might affect the physical and mental development of minors is allowed only for adults... The aim is therefore limited to preventing minors from encountering, by accident or otherwise, material that might affect their physical and/or mental development.*

There is some significance, therefore, in a further distinction between activity by young Internet users which may be harmful and that which is merely undesirable. Undesirable material in this context is material of which people publicly disapprove because it may arouse feelings of disquiet, disgust or indignation, but which is without adverse consequences to the viewer. Material that is mildly racist or ethnically biased could fall within this category. Children are naturally curious and like to break taboos and indulge their fantasies. It can realistically be assumed that many young people will, at some stage, seek to use the Internet for disapproved purposes. It has to be said also, however, that for the vast majority, this usage will be short-lived and harmless.

However, there are areas of concern when considering the harmful effects on children of the misuse of the Internet. Harmful material can have effects on the emotions and behaviour of children. It can also affect their beliefs and value systems. Some of these effects are described below[3]:

- Behavioural effects

  The technology provides a ready facility for jokes, pranks and embarrassment. More serious damage can be caused, however, by technically proficient students, some of whom will enjoy great personal kudos from their cleverness and perceived power. Their more passive, less expert counterparts will frequently “enjoy” the results.

  Claims are sometimes made that the Internet is addictive. Some young people forego all kinds of activities to spend inordinate amounts of time on their PC’s. Most such “addicts” are hooked on game playing, hacking or “surfing the net”. Far more serious, however, is another potential source of addiction - pornography or violent material. Adolescents, intrigued by sites containing depictions and descriptions of activities they would not otherwise have access to, or even conjure up in their fantasies, may find themselves attracted to revisiting particular sites. Hate groups also appeal to aggressive and abused young people, especially when they justify their animosity with propaganda. Cults and sects attract, and even recruit, isolated and confused youngsters who are looking for certainty in their lives. All such “addictions” are obviously unhealthy as they inhibit and warp normal emotional development.

[2] Green Paper on the Protection of Minors and Human Dignity in Audio-visual and Information Services. European Commission document (96) 483, 16 October 1996

[3] Psychological service, Department of Education and Science

- Effect on beliefs values and attitudes
  A preoccupation with marginal, unpleasant material can often give rise to false and distorted beliefs about the world. Pornography, for instance, relies heavily on equating sexual gratification with physical and emotional abuse, and consumers of it frequently believe that the victims enjoy their torment or are unharmed by it. Propaganda is believed if it is accompanied by plausible arguments or satisfies individual emotional needs. Correspondence with others who share beliefs greatly adds to their credibility. The intellectual limitations, emotional liability, immaturity and inexperience of children and young people make them particularly vulnerable to all this. Engrossment in any medium will affect a person's values and attitudes. Children and teenagers can be particularly impressionable as they are still in the process of developing theirs. Intense use of undesirable material can create negative mind sets or exaggerate already established personality traits. Pessimism, personal antagonism, cynicism, unpleasant precocity, disaffection, diffidence, sexism, racism, intolerance and anti-social posturing are some of the possible outcomes.

3.1.4 Child pornography

Although there are many ways in which the Internet can adversely affect children, the Group focused on the issue of child pornography.

The Internet - a medium for distribution

It must be remembered that apart from the obvious damage to the children who are actually used in the making of child pornography, there are dangers in children getting access to material which may be pornographic, hate-based, violent or in some way threatening to the well-being of the child. This question of access will be discussed later in the Report. The Group is in agreement with those commentators who argue that the term "child pornography" is, in itself, not fully descriptive of what is involved. Assuming that the images are not computer-created, images of adults engaged in sexual activities with a child are nothing less than images of an assault on that child.

A major concern is, therefore, the ease with which pornographic material can be accessed, stored and disseminated on the Internet. There is a strong perception that the Internet has become a major factor in the development of paedophile rings world-wide and many recent convictions in the United States and in the United Kingdom have shown that the medium is being widely used by members of such rings, both to share experience and to traffic in child pornographic images. The dissemination of child pornography is causing major concern to the International Agencies engaged in the protection of minors.

Images of adults engaged in sexual activities with a child...

Irrespective of the routes used for disseminating child pornography the problem continues to be serious in Western Europe where major child pornography rings have been uncovered in Denmark, Germany, Italy, the Netherlands, Sweden and the United Kingdom. As these networks increasingly use advanced telecommunications technologies, making use of encryption and code names, they have become more and more difficult to uncover. In addition to activities between paedophiles, inappropriate direct approaches to children can, of course, occur through e-mail and IRC activity. Sadly, the Internet has also been used as a medium to advertise child-sex tourism, particularly in Asian countries.

...are images of an assault

Not Just A Picture

Images in a range of file formats can be stored on and transmitted between computers using the Internet. Such images can be created through scanning of photographs/slides or digital-capture on video at relatively low cost, converted into a standard image file format and displayed or transmitted to other like-minded individuals. Adult pornography can be modified with the superimposition of a child's head onto an adult body, creating an obscene image that is not in itself a representation of a specific act of abuse. While the quality of these images is sometimes poor, improvements in technology will facilitate such modifications. It might be noted that the "Child Pornography" Bill addresses the issue of computer- generated child pornography images.

Child pornography can also be audio or text-based

Although legal definitions tend to be explicit in their reference to overtly sexual images, it is in the area of context that its effectiveness will become more difficult to assess. The research presented to the Group by Professor Max Taylor notes the preponderance of images of children in paedophile traffic which cannot be categorised as intrinsically obscene or graphically sexual. He uses the term “child erotica” to characterise such material. Such images may not of themselves fall within the accepted objective definition of child pornography.

It must also be remembered that the Internet readily facilitates the storage and transmission of two other forms of child pornography; text-based material and audio-pornography. Today, the Internet is increasingly used by paedophiles to exchange graphic correspondence and to exchange knowledge and experiences. Audio pornography can be stored in digital files for transmission over electronic mail, displayed on a WWW site or can be posted to a newsgroup.

How is child pornography distributed on the Internet?

Newsgroups

We have already referred to the presence and nature of newsgroups in Section 2.2.3 of the Report. They are not stored in a single place but are copied between newsgroup servers. It is estimated that there are around 40,000 newsgroups currently on the Internet and the number is continually growing. There are also WWW sites which contain archives of many of the newsgroups, thus complicating what we may have considered to be boundaries between the various services. The Group was fortunate to benefit from studies carried out by one of its members, Professor Max Taylor and one of its specialist contributors, Rachel O’Connell from University College Cork. In relation to how paedophiles use newsgroups, their studies suggested as follows:

> *The name of the newsgroup will usually give a strong indication as to the type of content and there are several which are aimed at paedophiles. The content is usually text-based but encoded images can also be distributed through these forums. Text-based child pornographic material is easily accessible. It is notoriously difficult to estimate and track the amount of paedophile activity in newsgroups because of the orchestrated migratory nature of the newsgroup subscription by paedophiles.*
>
> *Research has suggested that paedophile activity in newsgroups is structured and organised by paedophiles in a co-operative manner. The organised migratory pattern that paedophiles adopt appears to offer a number of advantages. If subscribers to a child sex-related newsgroup feel they are being monitored they can move en masse to a different newsgroup. It is therefore more difficult to track the extent of paedophile activity when they keep moving to different newsgroups. It is also possible to miss newsgroups that contain child erotica and child pornography if the correct newsgroup names are not known.*

It is impossible to guarantee that blocking will work

Because newsgroups are stored locally by service providers and thereby subject to some degree of control, the issue of potential blocking of unsuitable material arises. This is a difficult issue which is not unique to the Irish situation and will be discussed in the context of the Group’s recommendations on new structures for the service provider industry. As in all intervention strategies relating to the Internet, it is virtually impossible to guarantee that a blocking intervention will be successful in the sense of guaranteeing the removal of targeted material. Blocking on the basis of the name of a newsgroup does not prevent another group with the same material being established or indeed that material being cross-posted to other groups with so called “harmless” names. As already pointed out, it is possible to access newgroups stored abroad by using the services of the local service provider to simply access the Internet.

Mailing lists

Mailing lists represent another problem area for child pornography activities particularly where subscription is by invitation only. It might be noted that in relation to "adult pornography", more centralised control of bulletin board systems permits operators to charge for their services. This opportunity for profit has motivated a number of pornographers to operate "adult" systems.

E-mail

Evidence from paedophile convictions indicates that e-mail is frequently used to distribute pornographic images. As already indicated, e-mail can contain text, images or program files and is a ready medium for the dissemination of illegal material. In the normal course, the name of the sender is contained in the message, but individuals concerned with avoiding detection can use anonymous re-mailer services which strip out these details before forwarding the message.

E-mail is frequently used to distribute pornography

Chat services

This "real-time" service offers paedophiles the opportunity to discuss their fantasies with others and to share experience in an anonymous context on the Internet. The main service, Internet Relay Chat (IRC) is also used to arrange face-to-face meetings. While most IRC sessions are public, private sessions are possible and there have been a number of reported instances of known paedophiles using such interactive sessions with children to gain their confidence before attempting to arrange meetings. A hybrid arrangement somewhere between e-mail and IRC is emerging in the form of ICQ services which allows private communication to take place in real-time mode between parties subscribing to a particular directory. These service are known to be used for paedophile purposes and are, because they leave no electronic footprints, very difficult to detect.

WWW

While initial research in the Group suggested that no unambiguous example of child pornographic material was readily available through the WWW, recent research undertaken in this area by Professor Taylor indicates that there is an increasing problem in this regard. Over 40 sites, mostly Japanese, containing photographs of naked female children were identified. Gaining access to additional photographs through these sites required either a password/controlled membership or access to a Bulletin Board, the address for which is provided. While indications were that contact with the Bulletin Boards in question was only available from Japan, video material offered for sale was available for shipping to Europe. The research therefore indicated a level of commercial activity not seen in Europe or the United States. In addition, at least one Japanese site facilitated the exchange of images for a fee.

A range of new technical tools is available which will make these activities more widely available and more easily produced. These new features include high quality video; virtual reality; on-screen video conferencing; faster data transfers; more powerful web design tools; more sophisticated search engines; increased security and more feature-rich browser software. Video conferencing, for example, would permit home-based computer users, with the help of miniature microphones and cameras to see each other live on-screen during their exchanges over the Internet and engage in child abuse in real-time mode.

Technology will facilitate exchanging paedophile material

The Group believes that these developments will provide greater means for the production, dissemination and exchange of material that is of interest to paedophiles. There is a concern that, on a practical level, the ease of copying and disseminating digitised child pornography presents unique law enforcement challenges because the seizure and eventual destruction of computerised child pornography may no longer appreciably reduce the amount of child pornographic imagery existing in the paedophile underground. In addition, in cases where the production of physical evidence in a court of law is required to successfully convict, the ability to totally erase material from computer disks represents a serious problem for those charged with law enforcement. While there is no case law in Ireland in relation to these issues, some examples of recent court cases abroad relating to paedophile activity are shown in Appendix 5.

3.1.5 The Internet and schools

A discussion of the issues regarding children and the Internet would not be complete without a reference to its use in schools. In a schools context, use of the Internet can enhance classroom opportunities dramatically by making available to students and teachers resources from all over the world, including original source materials. The Internet can bring information, data, images and even computer software into the classroom from places around the globe and it does so almost instantaneously.

Controls needed for schools Internet access

Access to these resources can stimulate individual and group projects, collaboration, sharing of curriculum materials and levels of idea sharing not found in schools that do not use the Internet. Internet access also makes possible contact with people from all over the world, bringing into the classroom experts in every subject area. Teachers and students can also create a Web Site as a source of information to be shared with others on the network. In using the Internet, concepts of class, race, gender, age, ability and disability have little significance and it is, therefore, a valuable tool for those seeking to address the learning needs of all students.

However, as with many other aspects of children's use of the Internet, appropriate controls are required. The dangers represented by unhindered open Internet access by children through schools must be clearly understood by parents, teachers and school authorities. The benefits to children from Internet usage are enormous but must be balanced by appropriate awareness and training programmes and an innovative use of a number of emerging options in the area of content filtering and site selection schemes. Specific recommendations in this area are discussed in Section 5.5.3

3.1.6 The extent of the risks for children

The need for a balanced view

Determining the extent of the dangers associated with children and the Internet is very difficult. The nature of the technology and the global aspect of the phenomenon does not facilitate precise measures. Levels of awareness of the nature of the Internet and its contents vary considerably from country to country and even within countries. There is a need for a balanced view. On the one hand we are presented with a view which suggests that the Internet is awash with child pornography, with its worst excesses available at the click of a mouse. On the other hand, there are those who minimise illegal and harmful material on the Internet and are not aware of the dangers for children in its uncontrolled use.

Irresponsible indifference and unsubstantiated moral panic are the greatest enemies

The reality, as in all aspects of human existence, lies somewhere in the middle and it is this balanced view which will maximise our efforts to understand and address the overall problem. Irresponsible indifference and unsubstantiated moral panic are the greatest enemies to ensuring that vulnerable users are adequately protected on the Internet.

The US experience

Against this background, it is worth examining some of the efforts which have been made to quantify the problem. What purported to be the first major academic study of the use of the Internet to disseminate pornography, undertaken by Rimm[4] and published in the Georgetown Law Journal, generated a storm of media interest when it was used as a basis for a Time Magazine cover story in March, 1995. Many of the more sensationalist contributions to the debate on the American Communications Decency Act (CDA) were based on the observations in this article.

Rimm produced statistics which suggested that paedo-hebephilic and paraphilic imagery accounted for 48.4% of all downloads from commercial "adult" bulletin board services. In addition, it was widely and inaccurately reported that the 'Rimm Study for Carnegie Mellon

[4] "Marketing Pornography on the Information Superhighway" study by Marty Rimm for Carnegie Mellon University, Pittsburgh, USA 1995. Published in volume 83, issue 5 of the Georgetown Law Journal. Available at http://trfn.pgh.pa.us/guest/mrstudy.html

University, Pittsburgh , had examined some 900,000 Internet images, finding over 84% of them to be pornographic. However, a number of academics have since claimed to have identified major flaws in his research methodology and in his assumptions. Many of the adult bulletin boards are commercially established to disseminate such material and screened subscription-based access is the norm. It is improbable that they could be found inadvertently. It is evident that while such material can be accessed, often at a cost, it is available in the main from special sites and newsgroups and its volume is low in comparison to other Internet content types.

The University College Cork study

In addition to indicating how child pornography was distributed (paragraph 3.1.4), this study also looked at the extent of child pornography on the Internet. It focused on the three principal areas of child pornography on the Internet; newsgroups, Chat (IRC and ICQ) and WWW sites. The main points of the study are shown below.

Accidental access to child pornography on the Web is unlikely

The amount of child pornography accessible through the Internet is considerable, but usually it is hidden or access is protected; the situation, however, is fluid and dynamic, with sites frequently changing addresses. Accidental access to child pornographic pictures on the WWW is unlikely, but using particular words (sometimes quite innocent words), as key words for search engines will yield access to child sex-related sites. Of course, the results from searches using these words will also yield many thousands of quite innocent sites. Links from such child sex-related sites are also an important source of further information enabling access to less obvious sites. Obscene text accounts of sexual activity with children are more readily accessed accidentally than pictures and in particular, underage boy-related accounts may be more easily encountered by accident.

Most of the child pornographic photographs and video clips that can be accessed on WWW sites have their origins 20 or 30 years ago. Recent pictures are less prevalent, although in the absence of a reference database, there can be no certainty of this. Text-based material is much more recent, as is child erotica. Photographs exchanged by e-mail, IRC or other messaging protocols may be more recent.

Paedophile activity on the Internet other than the collection of pornography is largely related to communication and the dissemination of information. Paedophiles are highly selective, with little cross-over between sexual interests in girls and boys; this distinction is largely reflected in Internet activity. Both e-mail, Chat and other messaging protocols are used to correspond, exchange fantasy and generally to provide mutual support. Specifically, information on secret WWW sites, discussions about suitable sex tourism countries and contacts, and general exchange of information takes place.

An example of a relatively structured support activity is a moderated mailing list, which is for “people to discuss their feelings towards young girls (i.e.: girls before their fourteenth birthday). It is intended to provide peer support, for those having difficulty with their feelings, for girl-lovers who feel isolated with their girl-loving, for those who possibly have no other avenue of discussion other than via the Internet. It is also intended for anyone else wishing to educate themselves about the nature of girl-love and girl-lovers”. This is similar to the newsgroup on boy-lovers, but operates as a private mailing list. There appears to be some Irish involvement in this activity.

Child pornography is posted on newsgroups

Child pornography continues to be posted in large quantities on newsgroups. While Irish Internet Service Providers may attempt to block access to paedophile newsgroups, it is possible for Internet users to use service providers merely as a conduit to get access to newsgroups held outside the jurisdiction. Research carried out during the first week of January 1998 suggested that there were in total 40,000 newsgroups, 0.07% of which contained major elements of child erotica and child pornographic pictures. These pictures amounted to 6058 in total, two thirds, of which depicted child erotica and one third could be described as pornographic.

Difficult to estimate paedophile traffic on IRC

All IRC networks continue to have channels devoted to both the exchange of child pornographic pictures, and to 'chat' related to fantasy and alleged sexual assaults on children. On 8 November 1997, a sample of activity on Dalnet showed 31 channels with titles related to child sex, with 281 participants. Channel names can be quite descriptive and ranged from "babysex" with 4 participants to "kinky preteensex" with 37 participants. A sampling of Undernet on that day showed 237 participants on 24 channels, with channel names ranging from "toddlerspanking" to "preteenboysexpics". In addition, there are an unknown number of private channels, and others, which do not indicate the area of interest by an obvious name. Access to these channels is often by invitation, and they are usually password protected. Due to the organised dynamic nature of paedophile activity it is not possible to estimate with accuracy the amount of traffic generated on IRC channels. At the time when this study was conducted there was no evidence of any active or consistent Irish involvement.

Other messaging and pager protocols are also used for the exchange of child pornography and information. ICQ (a 'phonetic acronym' of the statement 'I seek you') technology is based on a proprietary server and database network. It allows users to seek out other ICQ users and informs the inquirer of the "sought users" on-line status. Indeed it informs the inquirer when the "sought user" comes on-line in real-time. ICQ supports a variety of Internet applications and serves as a Universal Platform from which any peer-to-peer application (such as Microsoft NetMeeting or Netscape CoolTalk) can be launched. By routing all inter-user communication as peer-to-peer, information is transported in real time in virtual networks rather than routed via servers.

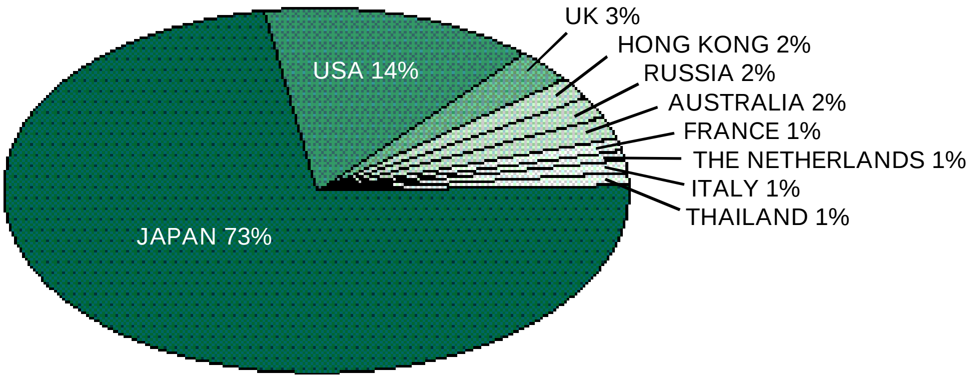
It is this peer-to-peer function that conceivably affords a further degree of security to users in the event of communicating sensitive information such as child pornography. In the absence of any explicit list, and without having appropriate contacts, the extent to which these protocols are used is unknown. This new technology demonstrates the versatility of Internet tools and the sophistication of the paedophile user. Internet tools and infrastructure are constantly evolving, and this emphasises the need for those researching the area of paedophile activity on the Internet to constantly monitor and keep aware of new developments which are shaping, and possibly being shaped by, deviant activity on the Internet.

Child pornography on WWW sites appears to be growing

The number of WWW sites involved in child pornography appears to be growing and complex networks of linkages relate sites to each other. Growth seems to be in the commercial area, centred on Japan. Over forty Japanese sites seeking payment for access to child pornography have been identified using search engines looking for appropriate key words. Without payment, sample censored pictures may be accessed on these sites illustrating the material available. On payment, a password is supplied to enable access to other pictures. A total of 12 sites offered videos or magazines for sale by mail order, with payment for 5 through credit cards. Videos were purchasable from one of these sites using a credit card. While the video would be posted in Japan, the credit card would be charged to a US company.

Secret WWW sites exist from which child pornographic pictures can be downloaded. The picture files are encrypted, with passwords, etc. circulated by e-mail. On one Japanese site, the picture files are changed weekly. The pictures include both “erotica” and pornographic pictures. The results of a systematic review of sites revealed 238 that have appeared between 18 June and 8 November 1997 offering access to girl-related child pornography or erotica. Boy-related sites are greater in number. The most sexually explicit sites are in Russia and Japan; however, it should be noted that the situation is very fluid, with established sites changing addresses, and new sites appearing. There is also a growing use of mirror sites that may disguise site of origin. Most of the pornographic photographs available from Japanese WWW sites are censored through the use of ‘masks’ covering the genital area. However, software is readily available which will remove the mask revealing the uncensored photograph.

The percentage of 238 sites of girl-related interest located in ten different countries is shown below:



Conclusions of study

- The general conclusion of the UCC study was that the Internet continues to be a major (if not the major) focal point for the distribution of child pornography and information about paedophile behaviour. Paedophiles can and do act cohesively as a group when on-line. Arrests in a variety of European countries and the US during 1997 suggest that computer collections of child pornography are commonly associated with paedophile activity.

- There is clearly a measure of organised commercial exploitation of child pornography in Japan, but less evidence of this was found in Europe, the only notable area being Russia.

- There is some evidence of Irish involvement in Internet activity related to child pornography and paedophile behaviour, although this is probably at a low level. In addition to the involvement noted above, there are occasional Irish participants on IRC channels, and occasional newsgroup postings from what may be Irish addresses.

The Internet continues to be a major focal point for distributing child pornography

3.1.7 The problem in Ireland

Great care is required in interpreting the limited amount of information available regarding the extent of the problem of illegal and harmful use of the Internet in any one country. It must be remembered that the Internet is global by nature and such material is, roughly speaking, equally available in all countries from an access point of view. This will change as access controls and internationally co-ordinated and agreed interventions expand and become more sophisticated. Formal intervention and "regulation" of the Internet is, however, a very sensitive issue and unbalanced and poorly-considered restrictions, apart from hindering the positive benefits of the Internet, can sometimes actually fail to achieve their objective. As this Report constantly stresses, an informed balance is needed, based on wide-ranging national and international co-operation. This will not be an easy task.

The "Internet in Ireland" is the same as in any other country

Arising from the nature of the technology, however, there is a certain uniformity of access to illegal and harmful material on the Internet which complicates the assessment of the situation in any one country. There have been some initiatives already from service providers in Ireland to block certain material on the Internet. Roughly speaking, however, the technology ensures that the level of access to the Internet by Irish subscribers is very much the same as the level of access from anywhere else in most western countries. It is not that the "Internet in Ireland" is in some way particularly vulnerable to paedophile activity. Taking into account the UCC research and the Group's own experience and study of the issue, we conclude that, no more than in other countries, a serious child protection issue exists in relation to the use of the Internet. It must be addressed.

A serious child protection issue exists and must be addressed

The Irish Society for the Prevention of Cruelty to Children completed and published its analysis of Childline calls in February 1998. However, the ISPCC have indicated that calls received indicate very little evidence of forced participation in or exposure to child pornography material by young people calling the service. Consultations by the Department of Health and Children representative in the Group with Health Board Care Workers failed to elicit significant evidence of such activity.

To date, there is no record of any prosecution within the jurisdiction relating to the use of the Internet to traffic in, or receive child pornography. However, the Group noted a reported increase in the levels of complaints to the Gardaí and the more active police role being adopted in this context.

It is reasonable to infer that in any society, an appetite for this material exists. The Group feel that there is no reason whatsoever why this country should be an exception in this regard. The nature of paedophile activity on the Internet suggests that it can continue undetected for a considerable period of time and it may only be in the context of a criminal investigation that it will come to light. While it is likely that the extent of this problem in Ireland is relatively limited in nature, it is equally likely that individuals are participating in child pornography exchanges, as yet undetected. The new structures proposed by the Group in Part 5 will, however, assist in determining the extent of the problem.

3.2 RATING SYSTEMS - A TOOL FOR THE FUTURE?

3.2.1 Fighting back with technology

The desirability of applying classification systems, such as those which operate successfully for film and video material, to Internet content has frequently been mooted, and the technology to facilitate this has been developed in recent years. Programs have been developed which operate in conjunction with Internet access software and are used to detect a rating or classification applied to the content either by the content provider or by a third-party service.

On the face of it, such tools represent significant progress in dealing with the downside of the Internet, particularly in the area of harmful content. If all material on the Internet could be classified, then a decision about what can be viewed could be controlled at an individual level so that parents, teachers and those involved with protecting the vulnerable members of our society could "filter" access to the Internet by filling in details of restrictions using special programs installed in their own PCs. Individuals could, of course, decide that they want no restrictions or that they want restrictions only for designated people-including children. While the Group is convinced that these tools provide some long-term solutions to the problems of the harmful use of the Internet, their development is at a relatively early stage and considerable work needs to be done, particularly at international level, before they become an effective reality. It must be said, however, that because of the urgency of the issue of child protection, they may represent important interim measures.

More work needs to be done on developing filtering tools

3.2.2 Rating systems: PICS and RSAC

Because they do form such an essential part of the overall solutions to Internet problems, the Group spent some time examining the various issues involved. There are two aspects to what is generally referred to as "rating systems". The first is the technical platform used to allow the filtering software to operate (it should be remembered that the Internet is empowered by a very wide range of protocols and rules-all of which must be able to "speak" to each other). There is, as yet, no agreement on what this standard platform should be. The leading contender is, however, a system called PICS and it is described in Appendix 6. As with all such major international standardisation, they are overlaid with substantial political, commercial and economic interests. Until there is agreement internationally on the adoption of a standardised rating system, the ad-hoc nature of its application may diminish its effectiveness.

The second aspect refers to the details of the system used for rating: how various types of material can be classified and encoded; e.g. levels of nudity, violence, racial references etc. Again, the current leader in this field is RSAC and details of this system are also given at Appendix 6. It is worth noting also that there is a definite American influence in these products and an input will be required from Europe to reflect other cultures and preferences.

European influence needed

One of the major problems arises from the need to decide on an overall system which is capable of reflecting the cultures of many countries all over the world whose traditional background and tolerance levels are so diverse. It can be seen therefore that international co-operation in this sphere is essential for any progress.

3.2.3 Existing products

In the meantime, it must be said that a wide range of products is currently available in the market which provides some protection for those who want to have some form of screening software. Their level of sophistication is, however, low and as the "European Action Plan on the safe use of the Internet"[5] points out, they are not very suitable to deal with European linguistic and cultural diversity. Appendix 7 describes this screening software in more detail.

3.3 THE INTERNET AND THE LAW

The Internet operates on an international basis. The law operates on a territorial basis. Thus we have the genesis of many of the legal issues surrounding the Internet. The link between the nature of the Internet and the way in which the law operates has already been referred to in Paragraph 1.5.1 and legal problems can, in many cases, only be fully understood through an appreciation of the technology and the way in which it works.

The Internet is international... the law is territorial

[5] Communication from the European Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions "Action Plan on promoting safe use of the Internet". Available at http://www2.echo.lu/legal/en/internet/actplan.html

There are a number of key legal issues which arise at national level. They include:

- the liabilities of the various parties involved in providing Internet services;
- the adequacy of existing laws in relation to illegal aspects of the Internet;
- our ability to develop new law which reflects the challenges posed by the downside of the Internet.

3.3.1 Liabilities

The question of legal liabilities often turns on the issue of the extent to which any particular party controls, or is aware of, illegal content. Users, content providers, service providers and telecommunications suppliers all have different levels of accountability ranging from direct responsibility to what is termed "common carrier status" reflecting no liability for content.

There are no simple answers on liability

Drawing the line
It is not the function of the Group to offer legal interpretations but we do feel that there must be a very clear relationship between legal provisions on legal liability on the one hand, and the different levels of control and knowledge in relation to illegal material on the other. For some of those involved in the Internet business, this line can be drawn quite clearly. For others, it is a difficult line to draw and particular issues may only find resolution in the interpretation of general law by the Courts. There are no simple answers and the nature of the technology presents real challenges for legal systems worldwide. Ultimately, liability can only be decided by the Courts in relation to the particular circumstances of each case. It must be noted that there are no known decisions of Irish courts on liability for communications on the Internet.

It is worthwhile remembering that there are different types of communications on the Internet, varying from e-mails (which can sometimes be the equivalent of private letters) to publication on web sites (which can be publication to the whole world). Bearing this in mind, if a particular type of communication is illegal off-line, then, as pointed out in Paragraph 1.5.1, it should be illegal on-line.

Packet-switched services
It would appear that value-added suppliers of packet-switched networking services (e.g. the X25 services which are provided by telecommunications suppliers world-wide) would not be responsible for the content of any such material transferred via such networks other than to co-operate with lawful requests for help from police in relation to criminal investigation. A possible exception, however, is where it is proved that a service provider continued to provide access to a specific piece of illegal material after being informed of its illegality.

The position of the Internet service providers (ISPs) is, however, much more complex. The services provided by ISPs also involve a type of packet-switched services and include access to non-local Web pages, e-mail services, IRC, file transfers using FTP etc. To the extent that any legal liability exists for accessing services over such kinds of networks, it would seem, therefore, to lie solely with the subscriber.

Service provider liability
However, some ISP services do rely on content which is stored on computers within the jurisdiction. Examples of such material are locally-stored Web pages and newsgroups. In simple terms, some services are provided using material held locally, and other services are purely access services relying on material held outside the country.

Even if liability were focused on whether or not material was stored within the jurisdiction, that is not the end of the problem. There is still the question of whether a service provider "knew" such material was being stored, given the scale and transient nature of the vast amounts of material flowing through Internet servers. In reality, there is no absolute way of knowing the full nature of all material held by service providers within the jurisdiction.

The "blocking issue" is about adopting feasible policies

The issue is not about guaranteeing the blockage of all harmful and or illegal material. The blocking issue is more about adopting feasible policies in this area which (a) are sufficiently discriminatory and effective so as to maximise the full benefits of the Internet, (b) are in conformity with legal provisions, and (c) respect, in particular, the protection and interests of children. The Group feel that this daunting task is best fulfiled in the context of a constructive partnership of all parties and an appropriate forum for common decisions on the many sensitive issues involved. Such a forum is recommended in Part 5.

New structures needed to address foreign Web Site issue

Access to foreign Web sites

A further difficulty discussed by the Group refers to the problem of ISPs inevitably providing access to illegal Web sites held outside the jurisdiction. After considerable discussion, it was accepted by the Group that there are serious technical difficulties in blocking access to such sites. The use of links within Web pages were seen as a further complicating factor. Emerging new technologies are also increasing the level of difficulty associated with tracing and blocking such material. As in blocking locally-held material, the same balance does, however, need to be achieved between the complex mixture of conformity with the law, technical feasibility, child protection and economic benefit. As already stated, this issue is best addressed in the context of the new structures proposed by the Group in Part 5.

The layers of complexity are further intensified by the fact that those same emerging technologies may well allow a user to access the Internet without going to the service providers in the State in which the person is situated. The general question of liability is, therefore, an issue which will not be resolved in the short term. The quality of "Internet sensitivity" of our national legislation will, however, be crucial to progressing the issue and this is a topic to which we now turn.

3.3.2 "Pornography" Bill

The Group were very glad to have the opportunity to discuss the Child Trafficking and Pornography Bill 1997 which was being developed in the Department of Justice, Equality and Law Reform at the time of the Group's deliberations. The discussions included the issues already referred to in Section 3.3.1 relating to liability and the challenges posed in ensuring that national law was "Internet sensitive". One of the most difficult aspects of the role of the service providers in this area was the degree of knowledge which they possessed in relation to the possession and distribution of child pornography.

The concept of "knowing"

While considerable progress was made on this issue, the Group feel that the liability of the service provider in particular cases is not capable of being resolved in advance of judicial interpretation of the legislation, on enactment. We accept that there can, in fact, be no guarantees for any party in relation to legal liability. Each party involved must make their own assessment of their position in this regard. We do, however, reiterate that the reality of providing Internet services in such a complex environment must inform all legislation which touches on these activities. It is acknowledged by the Group that the concept of "knowingly" introduced as a result of discussions between the Group and the Department of Justice, Equality and Law Reform will assist in protecting the ISPs in situations where the nature of the technology does not permit knowledge of content.

3.3.3 Future legislation

Future legislation must be sensitive to Internet technology

Discussions on the Bill did have a useful side-effect. It impressed on the Group the need for future legislation to be sensitive to emerging developments in Internet technology. The successful and safe use of the Internet is critical to many aspects of Irish society in the new millennium and legislative provisions which strike the balance between successful commercial exploitation of the Internet on the one hand and the protection of our children on the other, will be crucial. While there are concerns about liability which may only be fully resolved when the legislation is being interpreted, the Group feel that a good start has been made with the new legislation on child pornography.

3.3.4 Other Legislation considered

Given the attention which the Group decided to give to the emerging Child Pornography Bill, it was not possible for us, in this first Report, to carry out an examination of other legislation which touched on the issue of the illegal and harmful use of the Internet. However, a number of existing legal provisions were briefly noted as being of relevance for future examination:

- 1993 Interception Act:
  (The Interception of Postal Packets and Telecommunications Messages Regulation Act 1993) In relation to paedophiles making contact with children on the Internet, the Group considered whether the existing power to intercept telecommunications messages was adequate for the detection of such cases. The 1993 Interception Act provides for authorisations, subject to certain conditions, for interception of telecommunications messages in the investigation of a serious offence. That would appear to cover cases where an offence of child sexual abuse has been, or is suspected to have been, committed or is apprehended but is not being committed. However in the absence of information suggesting that a paedophile might be prepared to commit further offences, the 1993 Act would not appear to allow the interception of the telecommunications message of a convicted paedophile merely on the ground that he was a convicted paedophile.

  Wider issues concerning the monitoring of convicted paedophiles are involved which are not limited to monitoring the Internet. In the absence of a more detailed examination of the issue, no recommendation for an amendment of the 1993 Act is being made at this stage.

- Video Recordings Act 1989
  The 1989 Video Recordings Act prohibits the supply of videos which contain, amongst other things, obscene or indecent matter which might deprave or corrupt persons looking at the video. The Act would, therefore, seem to apply where someone in the State supplied this kind of video over the Internet for reward. In the context of distributing Internet material to the public, it might be noted that the Prohibition of Incitement to Hatred Act, 1989 probably applies to distribution to the public of material in contravention of that Act.

  The matter will be further examined in the context of the Group's next report. It was noted also that the Video Recordings Act also covers material which would be likely to stir up hatred on grounds of race, colour, nationality etc.

US distinguished between obscene and indecent material

The Group noted that the US Supreme Court had upheld the constitutionality of the provisions of the United States Communications Decency Act, 1996 which prohibited obscene speech. However, the Court had drawn a distinction between obscene and indecent material and it held the prohibition of the 1996 Act on the dissemination of indecent material on the Internet to be unconstitutional.

- The Data Protection Act 1988

  The full implications of the Internet for personal privacy are only now beginning to be examined but there is no reason why the rights to privacy guaranteed in a non-Internet environment should not be continued for personal data held on the Internet. This legislation does, in fact, seek to reconcile the rights to privacy with other rights including the rights of access by law enforcement agencies. In doing so, it establishes appropriate procedures within which such agencies must operate. While information on the Internet is held in a much more complex and intricate way than in a conventional computer system, the basic principles enshrined in data protection would still seem to apply.

  The ease with which data can be communicated on the Internet generates an enormous amount of personal data through its networks. This personal data is sometimes collected and used without due regard for the fair obtaining principles enshrined in the Act. The personal data collected by whatever party, be it service providers, commercial businesses or individuals, must be treated in conformity with existing legislation in this area and with due regard to the rights of the individual concerned to control the subsequent use of that data. It is interesting to note that the European Union, quite apart from harmonising existing data protection law in a forthcoming EU Directive, is taking steps to specifically address the question of protecting privacy on the Internet and is preparing the ground for the production of guidelines in this area.

Basic principles of data protection should apply to Internet material

3.4 STRUCTURAL ISSUES

The current Internet environment is characterised by a number of factors which give rise to certain structural issues. These factors include; rapid technological change; the presence of a multiplicity of players, both private and public; the emergence of recent significant international initiatives; and an increasing level of Internet access which is generating a growing consciousness among the public of the presence of illegal and harmful material on the Internet.

3.4.1 New partnership and new structures needed

There is a further factor slowly emerging which the Group wishes to highlight. This refers to the fact that the downside of the Internet, irrespective of the different perspectives and interests involved, represents a common enemy which will only be defeated through partnership and co-operation. As outlined at the beginning of this Report, the phenomenon of the Internet is unique and present unique challenges. As such, it requires a unique response. Given the multiplicity of players, the international nature of the problem and the importance of finding a solution, the Group felt from an early stage that a special partnership arrangement will be required to meet the challenge. This will inevitably involve new structures.

Special partnerships needed for addressing downside issues

Absence of forum

There is no natural forum emerging to discuss or provide co-ordination on the wide range of issues which we have already identified. In the public sector, various Government Departments have a range of functions relating to different aspects of the Internet. Although the Department of Justice, Equality and Law Reform is, perhaps, the public body most associated with the Internet, the reality is that almost all Departments are affected. For example, the most important initiatives taking place at European Union level regarding the downside of the Internet are taking place in the telecommunications and the arts and culture area.

Emerging co-operation

In the private sector, competitive issues in a relatively small market do not facilitate the emergence of co-operative structures. It is an evolving environment characterised by rapid changes of ownership and a searching-out of added-value services including the development of niche markets. It must be said, however, that there have been positive signs of co-operation in recent times and the emergence of the Internet Service Providers Association of Ireland (ISPAI) has been a very significant development in this regard. The positive co-operation shown by the Association in the deliberations of the Working Group is an indication of how much can be achieved in a partnership arrangement.

The problem of co-operation and co-ordination is not solely a national one. Over the past year, the same multiplicity of players and activities can be observed at European Union level where discussion papers on different aspects of Internet developments have emerged and proliferated.

Counter-productive to "regulate" the Internet

Non-statutory approach favoured
While there is a need to ensure that any new arrangement will attract the co-operation of all parties, the Group do not favour the introduction of statutory structures. We believe it is not only impossible but also counter-productive to attempt to "regulate" the Internet in the sense of using national statutory provisions to control its illegal and harmful use. The defining characteristics of the Internet so far explored in this Report, do, we feel, reflect that belief. This is not to say that our national laws should not continue to take careful cognisance of the emerging technology.

Rather, we believe that a partnership approach, characterised by a willingness to see these issues as common problems, supported by Government and Industry, is the best way forward at this point in time. From the deliberations of the Group so far, we feel that such a willingness is, in fact, available and should be exploited.

All partners must be included
Structural changes must also reflect the various sectors of society which will continue to be affected by the downside of the Internet. While there are practical limitations as to the breath of representations available on any group or committee, primary interests in the area of education, children, law enforcement, industry and Government, must be represented.

3.4.2 A new look at censorship controls

The Group would like to draw attention to another structural issue which relates to the way in which the boundaries between conventional media are starting to become blurred. The physical distinctions between text, audio and visual materials have, up to now, defined and conditioned our approach to the regulation of material which might be considered to be illegal or harmful. We have separate legislation which controls publications, videos and films, some of which has its origin in the early part of the century. It was possible to exercise such control because material existed physically in the form of books, tapes, magazines and films etc. Possession, distribution, sale and importation were relatively easy concepts to conceive and reflect in our national legislation.

The Internet, however, makes no such distinction. Information can exist and can be distributed on the Internet in text, audio or video form. Films, books, magazines, videos all become as one, in the electronic highways of the Internet's networks. Indeed, the technology and infrastructure of broadcasting is also moving towards new relationships with the Internet and the traditional television set may well become the Internet interface of the future.

The Internet ignores traditional media distinctions

Against this background, the Group feel it is time to initiate a long term examination and review of the structures which underpin our censorship system. There is a possibility that separate standards will continue to emerge for each of the traditional media such as books, television, videos and films and separate standards again for Internet material. Given that Internet material encompasses all the other media, the scope for inconsistencies is enormous. While the task of reviewing these structures does not come within the ambit of the Working Group, the issue is an important one and will have to be tackled sooner or later as the technologies continue to converge. In the meantime, we feel that any new structures established in the context of the illegal and harmful use of the Internet, should at least reflect an acknowledgement of the issue.

3.5 THE AWARENESS ISSUE

A sense of perspective

The final issue which the Group wishes to address is the important question of awareness. The most recent report from the Information Society Commission[6] has, quite rightly, identified the issue of awareness as being crucial to the exploitation of all information and communications technologies, and in particular the Internet, by all sectors of society. Awareness of the downside of the Internet is equally important and must be informed by a sense of perspective and balance. The Group wishes to emphasise again that moral panic, based on a poor understanding of the Internet, is the enemy of positive progress in dealing with the issues being examined. Equally, there is a reality behind the dark side of the Internet which must be addressed just as there is a dark reality behind the human condition which must be faced. Our strength does not lie in ignoring or downplaying that reality but rather in acknowledging it and installing appropriate measures to deal with it.

Our strength lies in adopting appropriate measures to deal with downside issues

No systematic research has been carried out on public perceptions of the Internet in Ireland and views in this area are accordingly somewhat speculative and often based on media reporting. The media has a very significant and important role to play in informing the public perception of the Internet and coverage of the issues involved have depended and intensified over the past few months. Inevitably, the downside of the Internet tends to attract the more sensational publicity and people who have only a passing interest in the Internet may not have a balanced view of its opportunities and threats.

No matter how we achieve this balance of perspective about the Internet, the Group feel that it must be fuelled at every level by a commitment to take every feasible step to eradicate the scourge of child pornography.

[6] The Information Society Ireland - First report of Ireland's Information Society Commission, December 1997.

International Experiences

4

INTERNATIONAL EXPERIENCE 4

4.1 EUROPEAN INITIATIVES - A GATHERING MOMENTUM

In accordance with the Group's terms of reference, an assessment was carried out of international approaches to the problem of the illegal and harmful use of the Internet. It must be said that the level of international activity in this area has intensified dramatically over the past year as a growing consciousness of the downside of the Internet has developed.

From the outset, the Group concentrated on assessing the domestic issues as prescribed by its terms of reference and set about outlining the responses which seemed appropriate in an Irish context. In parallel with this activity, the international subgroup examined developments abroad. Having brought these two dimensions together, it emerged that the main thrust of our initial recommendations were in line with emerging international developments - particularly in the European Union.

It has been constantly emphasised throughout this Report that the issues involved are essentially international and that the experience and ideas of other countries are acutely relevant to any national plans for an overall strategy. While a general consensus on approaches to the problem is now emerging, this has only come about in fairly recent times. Indeed, European initiatives which focus on pragmatic co-operative measures are only now emerging and countries within the European Union are at different stages in terms of their response to the illegal and harmful use of the Internet. The various threads are, however, now being drawn together.

International experience is crucial for developing national strategy

The need for international co-ordination and co-operation has never been greater. New ways of working together are needed which reflect the nature of the problems we are facing. It is interesting to note that the European Union are now talking in terms of an international "Charter"[7] to represent the kind of flexible and dynamic process which will be required. This Charter would not be legally binding but would be a multi-lateral understanding on how to co-operate to remove defined obstacles to progress. It would also permit participation by the private sector and relevant social groups.

4.2 GOVERNMENTS RESPOND DIFFERENTLY

Taking a more global view, as we must in terms of the nature of the Internet, not all Governments relish the prospect of untrammelled freedom of communication and expression for the individual. For some Governments, unfettered access by its citizens to the Internet constitutes an unacceptable political risk and access is therefore banned, confined to an elite, or otherwise subject to close control. Others recognise the benefits conferred by the Internet, but nonetheless wish, for political reasons, to place limits on access. Still others have very little concern about the illegal and harmful use of the Internet.

Child pornography is causing the most concern

In countries with democratic institutions and legally enshrined rights to freedom of expression, there is a positive appreciation of the new opportunities for communication and information/exchange offered by the Internet. Their Governments, like most, are however, also concerned at the ease with which the Internet can be used for illegal and harmful purposes; communication and the exchange of information by terrorists; opportunities for criminals to plan illegal activities; money laundering; fraud, etc. It is, however, the ease with which pornographic images, particularly those involving children, may be disseminated which is causing the most immediate concern.

[7] Proposal from EU Commissioner Martin Bangemann at Telecommunications Conference, Geneva September 8 1997.

4.3 AN INTERNATIONAL OVERVIEW

At one extreme, official Government policy dictates that the Internet is not available at all. Such countries would include Saudi Arabia, where it is perceived as a threat to religious and cultural values. Others in this category, such as Iran, make off-line access available under strict control to those deemed to require it. China recognises the value of the Internet and allows private Internet Service Providers, but insists that they obtain access through the relevant State Agency and operate other controls. Material from certain sites is blocked by the State Agency, for political or moral reasons. Persons with Internet accounts must register with the Security Authorities and certain services, such as newsgroups, are blocked. Skilled users in such countries can, however, if willing to take the risk, usually circumvent the restrictions.

In a number of other countries, particularly the newly-emerged democracies of Central and Eastern Europe, including Russia, controls are not exercised. The spread of on-line access is relatively recent and the authorities often do not have the resources to address the downside issues. Many developing countries are in a similar position. In India, the ISPs are legally responsible for ensuring that objectionable material is not carried. In practice, however, it is not been found possible to enforce this.

In the long established democracies with well-developed economies (broadly speaking the OECD Countries), there is, as already noted, with certain exceptions, a general concern at the abuse, and the further potential for abuse, of the Internet. There is, however, still considerable variation in the level of public and Government concern, depending on legal traditions and social mores. In Europe, this concern received a strong impetus from the paedophilic activities and child deaths which were revealed in Belgium in the Summer of 1996.

US are committed to making the Internet safe for children

In the USA, as noted earlier, this concern had already led to legislation in the form of the Communications Decency Act, which was incorporated in the Telecommunications Act, signed by President Clinton in 1996. This provided that the display or transmission of “indecent” material in “a manner available to minors” would be subject to heavy penalty. The strong concerns which led to this Act were, however, matched by concerns at the implications for freedom of expression. The legislation was immediately challenged by Civil Liberties Groups and industry interests and referred to the Supreme Court. On 26 June, 1997, the Supreme Court ruled that portions of the Communications Decency Act addressing indecency are not constitutional. In its reaction, the US Government has committed itself to studying the opinions of the Supreme Court closely and to making the Internet safe for children. It is understood that further initiatives in this area will be considered during 1998.

On 16 July, 1997, President Clinton and Vice-President Gore announced a strategy for making the Internet “family friendly”. It is interesting to note that in the context of this initiative, US industry commitments included the following:

- over 90% of WWW browsers will include filtering technology;
- major PC manufacturers and Internet service providers serving 85% of all Internet users will provide filtering software;
- Internet companies are promoting the use of ratings for filtering technology.

Technology is no substitute for parental involvement

The Group are in full agreement with the views of the President when he challenged parents to get involved with their children’s use of the Internet. “Technology”, he said, “is not a silver bullet and is no substitute for parental involvement.”

Belgium is concentrating its efforts on developing measures aimed at combating the sexual exploitation of minors via the Internet. Consideration is being given to the drafting of a Code of Conduct for Internet providers and for the establishment of a contact point for the detection of information of a paedophilic nature.

In France, a number of studies have been undertaken with regard to content on the Internet. The French authorities had considered making existing legislation more explicit in relation to the scope of responsibility of actors on the Internet. However, this amendment was not ultimately introduced.

The Federal Government of Germany adopted an Information and Communication Services Bill, on 1 August, 1997. This multimedia law is a general regulatory framework relating to the information society in Germany and includes provision governing the responsibility of service providers.

The United Kingdom has taken very definite action in this area through the establishment of the Internet Watch Foundation (IWF). This organisation resulted from a co-operative agreement between the Department of Trade and Industry, the Police and the Internet Service Providers. The organisation performs two functions:

- Running a public reporting line to allow members of the public to report the existence of material on the Internet which they find to be offensive or suspect to be illegal;

- Encouraging the rating and filtering of material on the Internet.

The priority of the Foundation is in tackling the dissemination of child pornography. The organisation has been successful in working with service providers to remove harmful material from their servers. However, the much wider problem of material being made available outside their jurisdiction is an issue which, they say, cannot easily be addressed by the Foundation. For this reason, a large part of their focus is on the area of rating and filtering and a special group has been established to prepare specifications of what should be covered in such a rating system.

The UK has also taken the lead in forming a consortium of non-Governmental organisations in Europe to focus on some of the issues of self-regulation. This is European Union part-funded. It is interesting to note that the Internet Watch Foundation was funded privately by the former Chairman of the United Kingdom Internet Service Providers Association.

In Denmark, the authorities regard the Internet as a user-controlled carrier medium, unlike the broadcasting media. Internet Service Providers are not responsible for the content, although they are obliged to report illegal material as they become aware of it, and acknowledge this obligation. Pornography, apart from child pornography, is not illegal.

In Norway, ISPs may be held criminally responsible for disseminating pornography. ISPs have sought to protect themselves by agreeing to a voluntary code committing themselves to do what they can to block illegal material. A similar situation exists in Iceland.

In Finland, which has the highest per capita level of Internet access in the world, the approach of the authorities has been to seek to make legislation on the transmission of illegal material “machine neutral”. A Committee on Freedom of Speech Legislation reported in February, 1997 and among their recommendations is the designation of an ISP Manager as a “responsible editor” and therefore potentially liable to prosecution for the transmission of illegal material.

In Austria, the Minister of the Interior has been requested to take measures to prevent access to data which encouraged crime. Existing police laws allow the police to order criminal content to be taken off the Internet and there is a hotline in existence which allows citizens to report criminal content.

In Luxembourg, there is at the moment no restriction on ISPs but some follow a voluntary code of practice. A Working Group is looking at the situation.

In Italy, there is no specific legislation to deal with pornographic or paedophilic material on the Internet, although there have been attempts by Parliamentarians to promote the introduction of such measures.

In Spain and Portugal, there is some public and political concern, but no organised consideration has been given to the matter. In these countries, Internet use is not yet as widespread as in others.

The Japanese approach emphasises freedom of expression over regulation of the Internet, and regards the user as responsible for protecting himself from harmful material. An Association has been established to develop protective software.

In Korea, the sale, distribution and possession of obscene material is prohibited. The extent to which this is effectively enforced in particular in respect of the Internet, is not clearly established. There is, however, public concern, and the authorities are planning to distribute blocking software freely to the public.

In Australia, which shares many of Ireland's cultural values, the Federal (Commonwealth) Government announced principles for a national approach to regulate the content of on-line services such as the Internet on 15 July, 1997. The Scheme involves:

- A self-regulatory framework for on-line service providers;
- A sanctions regime;
- A framework that will not hold on-line service providers responsible for the content accessed through Internet services, where the on-line service provider is not responsible for the creation of that content;
- Encouraging the co-operative development of uniform State and Territory provisions regulating on-line content users.

4.4 THE EUROPEAN UNION

As already pointed out, the issue of co-ordination between a multiplicity of parties is not confined to national scenarios. The European Union are also facing the problem of adopting a co-ordinated approach and indeed, there are co-ordination requirements also between the European Union itself and other international organisations such as the Council of Europe and the OECD. In relation to the European Union, many specific law enforcement issues require examination in the context of Justice and Home Affairs (Third Pillar). Other initiatives in relation to the illegal and harmful use of the Internet are emerging from the economic (First Pillar) side of the European Union.

4.4.1 Justice and Home Affairs

The Stop Programme

The focus of the Justice and Home Affairs activities still remains on the criminal law and co-operation between police and judicial authorities. Of particular interest to Ireland is research being carried out under the STOP Programme initiated by Ireland during its presidency. This provided for measures to counter the use of the Internet for illegal activities such as child pornography and incitement to racial hatred. This programme, partially funded by the European Commission, must be of a European interest and include a grouping of EU member states. There are two Irish programmes involved. One is being led by Professor Max Taylor who is a member of the Group. The other is being carried out by Focus on Children. Both projects have a dimension which embraces an analysis of the extent and nature of child pornography on the Internet, including any Irish involvement.

Joint Action on Drugs

In December, 1996 a Joint Action on Drugs was adopted in which there is an explicit call for measures to counter the use of modern technologies, including the Internet, for the dissemination of information aimed at inciting others to produce or use narcotic drugs.

Action Plan

The European Council at its meeting in Dublin on 13 & 14 December 1996 underlined its absolute determination to fight organised crime and stressed the need for a coherent and co-ordinated approach by the European Union. It set up a High Level Group which drew up a comprehensive Action Plan containing thirty specific recommendations with realistic timetables for carrying out the work. It urged the Council and the Commission to take effective and coherent action "to address the abuse of new communications technologies, including the Internet" and noted the need to co-ordinate Third Pillar action on abuse of the Internet. The Action Plan to Combat Organised Crime was approved by the Justice and Home Affairs Council of Ministers in April 1997 and was subsequently endorsed by the Amsterdam Council in June 1997.

Reflection Exercise

Within the structures of the Justice and Home Affairs Council, a "reflection exercise" on the Internet issue is also taking place. This is aimed at developing practical co-operation among the law enforcement authorities about Internet-related activities including examining the adequacy of members states' legislative provisions and the drafting of law enforcement requirements for the information of the service provider industry.

Working Groups

Specific Working Groups are in place examining the question of the lawful interception of Internet telecommunications. The Commission is involved in the implementation of the Action Plan to combat organised crime endorsed by the European Council in Amsterdam. This includes a recommendation to combat the criminal use of new technologies and means of communication. The UK, in their role as President of the Council of the European Union and the G7/P8 during the first half of 1998 will endeavour to maximise the benefit of the shared expertise and experience of both fora in the fight against organised crime including that carried on through the medium of modern technologies (see Paragraph 4.5.5).

Fraud and Counterfeiting

Another recommendation invites the Commission and the Council to address the issue of fraud and counterfeiting relating to all payment instruments including electronic payment instruments.

4.4.2 Other European Union Initiatives

Telecommunications Working Party
The theme of “illegal and harmful content” initiated in the telecommunications area, has been debated and progressed through the various levels of the European Union. A Communication to the European Parliament in late 1996, set out proposals from the Commission for immediate action to deal with harmful and illegal content.

The Telecommunications Council agreed to extend the Working Party established previously to include representatives of the Ministers of Telecommunications as well as access and service providers, content industries and users. The Council asked the Working Party to come up with concrete proposals to combat illegal use of the Internet. The first Report was submitted to the Council in late November, 1996.

A Council Resolution on illegal and harmful content on the Internet was adopted in February, 1997. The Council welcomed the Report of the Commission Working Party and invited Member States to start work in a number of relevant areas. They asked the Commission to foster co-ordination at community level of self-regulation and representative bodies, to promote and facilitate the exchange of information on best practice, to foster research into related technical issues, and to consider further the question of legal liability for Internet content.

In April, 1997, the European Parliament adopted a resolution on the Commission Communication on illegal and harmful content on the Internet”. The resolution contained a list of desiderata addressed to the Council, the Commission and the Member States. The resolution emphasised the concept of self-regulation at European Union level and it encouraged enterprises and industries involved in telemetric networks to develop message protection and filtering software - to be made available automatically to subscribers. It also suggested that appropriate arrangements for making sure that all instances of Child Pornography uncovered on computer networks were reported to the Police and shared with EUROPOL and INTERPOL.

With regard to harmful content, the resolution stressed the need for the development of a common international rating system compatible with the PICS protocol and with sufficient flexibility to accommodate cultural differences among the Member States.

Green Paper
A Green Paper[8] was adopted by the Commission in October, 1996, at the same time as the Communication on illegal and harmful content on the Internet. This Paper addressed the need for regulatory frameworks in the context of the emergence of new audio-visual and information services. The particular focus was on the protection of minors and human dignity.

The latest development in this area takes the form of a proposal for a Council Recommendation on enhancing the competitiveness of the European Audio-Visual Information Services Industry by promoting a high level of protection of minors and human dignity. The title of the proposal is an interesting reflection of the close relationship which exists between competitiveness and the whole issue of providing protection with regard to the downside of the Internet.

In essence, the proposal repeats many of the agreed objectives regarding complaints handling, self-regulation, and the need for increased awareness in relation to illegal and harmful use of the Internet. It goes further in that it documents common guidelines for the implementation at national level of a self-regulation framework for the protection of minors and human dignity in on-line audio-visual and information services. This is of particular interest in the context of the Group's recommendations in Part 5 and a copy of these draft guidelines is shown in Appendix 8.

[8] The Green Paper on the Protection of Minors and Human Dignity in Audio-visual and Information Services. European Commission Document (96) 483, 16 October 1996.

The Green Paper and the Document on Illegal and Harmful use of the Internet together represent a significant contribution to the whole issue of the downside of the Internet. They are detailed documents and while they are meant to be complementary, there is considerable and inevitable overlap between them. They do, however, reflect a broad agreement between the European Parliament, Council and Member States on the general approach to be taken. If they are juxtaposed with the latest co-ordination mechanism issuing from the Commission relating to an Action Plan on promoting the safe use of the Internet, then, considered together, they represent the kernel of future national strategies over the next few years.

Key areas
All these international documents identify a number of key areas which offer feasible approaches to what this Report has argued is a difficult and complex problem.
They include:

- The need for self-regulation and co-operation between industry (access and service providers), political decision makers and users associations;
- The encouragement of content filtering and rating systems taking into account Europe's cultural and linguistic diversity;
- The establishment of complaints mechanisms;
- The need for awareness campaigns highlighting the drawbacks of the Internet, particularly for certain target groups.

In summarising developments to date, the Action Plan[9] states:

> *The intense activity of the European Institutions in this area since 1996, the political direction given by the European Parliament and the Council, the Ministerial Declaration resulting from the Bonn Conference and the developments in Member States show that Europe has, in many respects, been a pioneer in addressing the issues and proposing solutions based on industry, self-regulation, filtering and rating, and increasing user confidence through awareness... the fight against illegal content needs industry co-operation in restricting circulation and a fully functioning system of self-regulation aiming at a high level of protection, which must go hand in hand with effective law enforcement by the Member States and Third Countries.*

International problem - international response
The full return on for these measures will, of course, only come into operation when each Member State has established its own regulatory framework and complaints systems in association with general European-wide guidelines. The co-operation between European networks of hotlines envisaged by the Commission will, for example, represent real progress in addressing the issues described earlier in the Report regarding jurisdictions on illegal material. As already noted, the problem is international: The response must be international. The Group believes that a common European front is an essential pre-requisite to overall success in addressing downside issues.

Study on Liability
Finally, it is worth noting that the European Commission has published a call for tenders for a study on legal liability systems in Member States regarding information society services. The study will draw up an inventory of laws, regulations, administrative practices and forms of regulation which are in existence or in preparation in the Member States and which establishes forms of legal liability applicable to operators and users of information society services. First results are expected in early 1998.

[9] Communication document from the European Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions "Action Plan on promoting safe use of the Internet" Available at http://www.2.echo.lu/legal/en/internet/actplan.html

4.5 OTHER INTERNATIONAL INITIATIVES

4.5.1 U.S. International Conference on Cyber Crime

Ireland participated in a major Conference in February, 1997, in New York, hosted by the United States Attorney General, to bring together Legal Experts on Cyber Crime to examine what could be done on an international level. Confirmation that a high level of international co-operation was required was one of the conclusions.

4.5.2 Bonn Conference

The Federal Republic of Germany and the European Commission jointly organised a Ministerial Conference entitled “Global Information Networks: Realising the Potential”. This was held in Bonn, in July, 1997. The Ministerial Declaration from this Conference stated that:

> *Ministers stressed the role which the Private Sector can play in protecting the interests of consumers and in promoting and respecting ethical standards, through properly functioning systems of self-regulation in compliance with and supported by the legal system. Ministers encourage industry to implement open, platform-independent content rating systems and to propose rating services which meet the needs of different users and take account of Europe's cultural and linguistic diversity.*

4.5.3 Council of Europe

The Council of Europe Committee of Experts on Crime in Cyber-Space - (PC - CY) is dealing with Cyber-Space offences such as money-laundering, the offering of illicit services and breaches of copyright as well as offences involving attacks on human dignity and the protection of minors. The PC - CY is also dealing with Internet-related questions of criminal law to which a joint approach may be necessary for the purposes of international co-operation such as definitions, penalties and the liability of Cyber-Space operators including the Internet Service Providers.

4.5.4 OECD developments

The OECD has also taken action in these areas following initiatives by the French and Belgian Governments. In this context, the OCED have presented a “Report on Approaches to Content on the Internet”[10]. This Report provides one of the most comprehensive international summaries of approaches to content issues on the Internet and identifies that, in general, Governments include the following issues when developing their policies in this area:

- Defining main concepts in terms of the diversity of services and technologies available and identifying main actors in terms of the functions they perform.
- Clarifying liability and responsibility for various parties.
- Re-affirming the application of existing law to the medium,
- Respecting fundamental rights, common values and community standards,
- Recognising cultural diversity,
- Protecting special groups (especially children),
- Protecting privacy and personal data,
- Recognising intellectual property rights as a distinct category of content issues,

[10] Organisation for Economic Co-operation and Development (OECD) Document “Approaches to Content on the Internet” OECD Document ref DSTI/ICCP (97)14

- Focusing on technological solutions and the importance of the industry role,
- Focusing on education and empowering users
- Determining what international co-operation is necessary, what it would entail and how it might be accomplished.

It can be seen that, in essence, these approaches mirror the European Union initiatives.
The OECD Council of Ministers have also recently adopted a declaration strongly condemning the distribution of child pornography via the Internet and requiring immediate measures to fight these practices.

4.5.5 (G7 + Russia) / P8

A group of legal and technical experts in global networks was established in November 1996 following an initiative by the so called “Carnegie Group”. The aim of this Working Group is to create a catalogue of incidents of misuse of global networks and to propose solutions. The European Commission participates in the work of this group.

Also, the G7/P8 senior level group on transnational organised crime is working to develop legal and technical mechanisms to allow for timely international law enforcement responses to computer-related crimes. The European Commission will also play an important role in these discussions. In December 1997, the G7/P8 approved an action plan for combating the use of the Internet and other high-tech technologies for criminal purposes.

At their meeting in Washington, the G7/P8 countries agreed to work together to facilitate the work of the police and justice departments against organised crime on such networks. The declaration adopted provides for the installation of internal legislation that allows for computerised networks to be deemed to be criminal and to obtain, in good time, proof of crime. The declaration stresses that it is impossible for just one country to act alone against this problem, given the nature of modern communication networks. Progress accomplished in setting the action plan in place will be assessed at the G7/P8 summit in Birmingham in May next.

4.5.6 The International Communications Round Table

This organisation which represents thirty leading European, American and Asian companies adopted a resolution regarding illegal and harmful content on the Internet supporting the European Union initiatives in this field.

4.5.7 United Nations

The UNESCO has commissioned a feasibility study from the Australian Broadcasting Authority on initiatives being taken around the world in dealing with illegal and harmful content.

Responses to issues

5

RESPONSES TO ISSUES 5

5.1 INTRODUCTION

5.1.1 The need for national action

A consideration of Internet issues by the Group highlighted one very important facet of national policy development which will definitely be intensified into the new millennium. This relates to the degree to which our national responses to what might appear to be national issues are conditioned by forces and developments outside our jurisdiction. In the case of the Internet, such forces are driven by a technological phenomenon which allows for no borders and disregards many attempts to replace those physical borders with artificial technical controls.

Within this international expanse, there are however some major groupings. The United States exerts a powerful influence in terms of the volume of US-originated material on the Internet and has the ability to influence the software developments which drive the many services, controls and development tools surrounding the Internet. Developments in the browser market are a case in point. The main browsers, Netscape and Internet Explorer account for the vast bulk of the browser market.

The other major grouping to which we in Ireland are associated is, of course, the European Union and the wider area represented by OECD. As a block, and as described in Part 4, a series of co-ordinated initiatives is beginning to emerge which themselves will need to be linked to US developments. Countries outside these two main groupings do not appear to be major players in shaping the future of the Internet, at least in the short term.

Despite the background of this potential limitation, the Group believes that there are practical steps which can, and should, be taken in the short term by this country to address the downside issues posed by the Internet. It is not question of letting international developments further mature before taking action. Neither is it a question of directly copying all international developments. There must, however, be a general congruence between what infrastructural development takes place in Ireland and the general direction in which the European Union is progressing.

Practical steps should be taken in the short term

5.1.2 Criteria for Group's recommendations

There are a number of criteria which guided the Group's final recommendations regarding an appropriate response to the illegal and harmful use of the Internet. That response should:

- Reflect practical measures which can be implemented in the short term;
- Be capable of directly addressing the issue of child pornography;
- Be compatible with the overall national objective of extracting maximum economic and social benefit from the Internet;
- Be geared to the particular economic, legal and social conditions in Ireland;
- Be capable of being integrated with ongoing international developments.

5.1.3 Main areas of recommendations

Against this background, the Group proposes a package of strategic measures which focus on four distinct areas:

- The introduction of a system of self-regulation by the Internet service provider industry to include common codes of practice (COPs) and common acceptable usage conditions (AUCs).
- The establishment of a complaints hotline to investigate and process complaints about illegal material on the Internet.
- The establishment of an Advisory Body to co-ordinate measures so as to ensure a safe Internet environment within the self-regulatory framework.
- The development of awareness programmes for users which will empower them to protect themselves, or others in their care, from the illegal and harmful material on the Internet.

5.2 SELF-REGULATION BY INDUSTRY

5.2.1 The most appropriate approach

Self-regulation... a key building block for a national strategy

The Group believes that the introduction of a self-regulation framework is the key building block of a national strategy for addressing the downside of the Internet and accordingly recommend that such a strategy be pursued as an immediate priority. It must be stated quite clearly that the Government has ultimate responsibility for the welfare of its people in relation to the illegal and harmful use of the Internet and must ultimately take whatever steps are necessary to ensure such protection. However, given the inherent nature of this particular problem as already described in this Report, and the international trends in this area, a self regulation approach is, we believe, most appropriate.

While the constituents of that self-regulation framework may have elements which are the responsibility of particular parties such as service providers, the overall maintenance and development of the framework should be carried out by a representative forum which embraces all those with primary responsibilities in this area. This will be discussed later in Section 5.4.

5.2.2 Codes of practice

One of the most important elements in an overall framework of self-regulation is the development of codes of practice by the key players. This has already been done by Service Providers Associations in Australia, Canada, Denmark, Korea, Finland, United Kingdom and Japan. It is possible that, over time, a number of codes of practice may be applicable to an environment which is constantly changing and where new players are continually being introduced. However, the Group feel that the most important and immediate priority in this area is the development by the Irish Service Providers of common codes of practice governing the provision of the services which they provide. We are glad to report that in the context of the deliberations of the Working Group, the Internet Service Providers Association of Ireland (ISPAI) committed themselves to developing a number of common measures, including codes of practice, as part of a framework of self-regulation.

The nature of the codes

SP's should take ownership of the codes

The ISPAI have committed themselves to completing these codes by the end of July 1998 and the Group feel that work already carried out by corresponding associations of service providers in Europe will be relevant to the finalisation of the Irish codes. While it is important for the service providers to take ownership of the codes themselves, we recommend that the codes of practice reflect the criteria for the Group's overall recommendations as set out in Paragraph 5.1.2. and should include the following dimensions:

- The promotion of awareness of safety issues particularly those relating to the use of the Internet by children.
- A common approach to how existing and emerging filtering software can be presented and made available to the users.
- Procedures for interfacing with the other players in a self-regulation environment (Gardaí, other service providers, complaints hotline, etc.) and agreements regarding steps to be followed arising from such interfacing.
- Procedures for monitoring and ensuring compliance with the codes including sanctions for those who fail to comply.

Sanctions for non-compliance

The question of sanctions for non-compliance with codes is a difficult issue and the Group considered whether or not it was feasible to use the existing regulatory framework attached to the value-added service role of the service providers. Having consulted with the Director of Telecommunications Regulation, the Group decided against this particular approach as the focus of such regulation only relates to content issues. Sanctions will, nevertheless, be required to ensure compliance with the codes and the full co-operation of the industry will be needed in this regard.

5.2.3 Acceptable Usage Conditions

The relationship between service providers and their clients is a critical one in the context of safe use of the Internet. Service providers find themselves in a wide range of relationships vis-à-vis the users of their service. There is a need for clarity regarding the rights and duties of both parties. In an environment geared to user safety on the Internet, situations will inevitably arise where constraints are placed on users in order to fulfil the overall safety objectives established by the new structures. The development of acceptable usage conditions (AUCs) is an essential element in ensuring transparency and addressing the legal and economic dimensions of providing Internet services. The Group recommends that such agreements be established (whether or not as part of the codes recommended in Par 5.2.2) by the providers and notes the commitment of the ISPAI to this approach. Within these common agreements, provision should be made for removal of services from those in breach of the AUCs.

5.3 NEW COMPLAINTS HOTLINE

5.3.1 Non-statutory basis

Apart from codes of practice and general co-operative agreements between the players involved in self-regulation, new structures are required to support the new framework. The Group recommends the establishment of a complaints hotline to process and investigate complaints from users about illegal content on the Internet. We have already argued the case for the new structures to be non-statutory in nature and the complaints agency should be no exception in this regard.

A hotline to investigate complaints about illegal material

5.3.2 Functions of hotline agency

The new hotline should be headed by a Director and staff whose experience and background reflect the particular functions assigned to it.

These functions should include:

- The investigation of complaints from Internet users about illegal material on the Internet.
- The taking of appropriate measures to address identified illegal material hosted, posted or provided within the Irish jurisdiction on the Internet, in collaboration with all the relevant national players, including the Gardaí.
- Where illegal material is identified but is outside the jurisdiction, to follow agreed local blocking procedures where feasible, and to liaise with the appropriate national jurisdiction.
- In relation to harmful material on the Internet, to encourage, promote and assist in the development of rating systems for Irish sites in the context of emerging international developments in this area.
- To disseminate information about the hotline service to the Internet user community and to develop user friendly and effective methods for notifying complaints.
- To actively co-operate with similar complaint bodies outside the jurisdiction in the area of exchanging information and experience in all matters relating to its functions.
- To document and implement transparent standards and procedures for its complete range of functions.
- To publicly report on its activities at regular intervals.
- To report to a new Advisory Board on the Internet (see Section 5.4) on all matters which require advice, discussions or decision by the Board, including new Internet developments which the Director feels should be brought to the Board's attention.

5.3.3 Investigation of illegal material

In confining the functions of the hotline to the investigation of illegal material, two distinctions previously discussed in the Report must be kept in mind. The first distinction relates to the difference between illegal and harmful material; the second relates to whether or not the material is held within the jurisdiction. In relation to illegal material stored within the jurisdiction, steps can be taken to have it removed either voluntary by the service provider or, by default, through the law enforcement authorities. If illegal material is held on Irish websites, then the issue is relatively straightforward and can be tackled through agreed procedures.

Illegal material held on locally-held newsgroups are a different matter. In most cases the illegal material will have been posted from abroad, but liability issues arise once the material is held within the jurisdiction. As discussed in Section 1.5.1, the nature of the technology allows no easy solution to this issue. The Group is aware that individual service providers have already taken particular initiatives on blocking newsgroups or newsgroup material and it is possible they will continue to do so for a variety of legitimate commercial, legal or social reasons.

Having considered the matter, the Group does not feel that they are in a position to make a specific recommendation on the question of newsgroup blocking nor would it be appropriate for us to do so. We do feel, however, that the most successful overall solution to this particular issue will be found in an approach which capitalises on the new co-operative structures which we propose and which has, as its objective, a heightened awareness by all parties of the dangers involved. Such an approach would be best developed in the context of the deliberations of the proposed Advisory Board and the Group recommends that this matter be included in the examination proposed in (c) below.

New structures will address newsgroup blocking issue

Illegal material stored outside the jurisdiction represents a totally different scenario. The role of the Service Provider is confined to one of providing access. The issue then centres around the ability to “block” access and involves very complex legal and technical considerations already described in the Report. The extent of this problem will diminish as international co-operative measures continue to intensify. International expert opinion suggests that the ability of the service provider to block foreign illegal websites is both limited in its scope and unpredictable in its effectiveness.

This is not to suggest that nothing can, or should be done, in this regard. The Group recommends that (a) the complaints hotline should make the appropriate international contacts to request its removal (b) the hotline should be active in pursuing general education and awareness measures to alert users to the issues involved and (c) as a matter of priority, the proposed Advisory Board (Section 5.4) should arrange for a full assessment to be made of the technical options available for blocking foreign websites and the implications of adopting those options. The results of that assessment could, if agreed, then be incorporated into the service providers’ code of practice.

On the question of the extent to which the hotline should be proactive in its examination of the illegal and harmful use of the Internet, the Group feel that its role should, in the short term at least, focus on processing complaints. The question of a more proactive role in seeking out illegal content or in monitoring the accurate use of content ratings could be reviewed in the light of ongoing experience with the new structures.

A more proactive role for the hotline is possible in the future

5.3.4 Investigating harmful material

With regard to harmful material, the hotline has an indirect role. While decisions as to whether material is illegal will ultimately only be taken by the Courts, there is no such forum for assessing harmful material. Indeed, its subjective nature makes consensus on its effects difficult to achieve. Individual initiatives by individual service providers in moving or blocking harmful material, quite apart from the possible legal implications, would involve them in decisions in which they have no particular expertise. The establishment of codes of practice, the closer relationships between all the parties anticipated by the new structures, and the work of the hotline in the area of rating systems will, in any event, facilitate productive discussions on issues relating to harmful use.

Ultimately, the most appropriate response in the case of harmful material is for users themselves to be empowered to take decisions on their own behalf (or on behalf of those under their care), about the harmfulness of the material. In the longer term, this individual empowerment will come about through internationally-agreed rating systems with appropriate supporting tools. In the short to medium term, the hotline should do all in its power to facilitate the acceleration of such developments including an assessment of the particular requirements of a rating system for Irish sites so that Ireland can participate fully in international developments in this area.

Tackling harmful material ultimately needs user empowerment

5.4 ESTABLISHMENT OF ADVISORY BOARD ON THE INTERNET

5.4.1 Overall co-ordination

The Group wishes to emphasise that a high level of co-operation will be needed in a self-regulating partnership environment. Progress in the battle to find a balance between the successful commercial exploitation of the Internet and the protection of children from illegal and harmful content will only come from a willingness to work in new and flexible ways which address the unique requirements of this unique phenomenon. The hotline will need policy advice and direction from a partnership-driven forum which, in addition to guiding the hotline, should itself monitor, control and promote the overall framework of self-regulation. To this end, the Group recommends the establishment of an Advisory Board representative of the key players needed to ensure the success of the self-regulation framework.

5.4.2 Composition of Board

The Group feel that the Board should be appointed by Government and should have an independent chairperson. The composition of the Board should reflect as wide a representation as possible, compatible with the practical need to work effectively. We recommend that the Board should include the following representatives:

- Service Providers
  As this Report has constantly emphasised, this group are key players and represent the primary movers through which safety on the Internet can ultimately be achieved. The effectiveness of their representation in the Advisory Board will be critical and in this context, the Group recommends that their representative association fully reflect all the organisations involved in providing Internet services. The effective contribution of the service providers on the Advisory Board can only be made through a representative model. In practice, therefore, our recommendation implies that all those involved in Internet service provision in the Irish market be affiliated to their representative association. Indeed, the success of the self-regulation framework itself will be very much dependent on an across-the-board commitment from all service providers and full support for their association will be a very pragmatic and positive expression of such a commitment.

- Censor's Office
  A considerable amount of expertise in the area of evaluating media content resides in this Office and given the rate of technological convergence in the various media, the Group feel that representation from this area will greatly facilitate the work of the Board.

- An Garda Siochana
  In the area of illegal material on the Internet, special co-operative relationships with the Gardaí will be required and their presence on the group is critical.

- Internet Users
  While the Group realise that no ready forum exists for Internet users in Ireland, we feel nevertheless that appropriate input from users is required. The existing consumer associations network may be a source for securing such a representative.

- Government
  The Government has an obvious and critical role to play in facilitating, supporting and assisting the development of the proposed framework. In the final analysis, irrespective of what mechanisms are used, it must shoulder the responsibility for ensuring that acceptable safety levels in Internet usage are achieved and that the law is, in fact, respected. Government representation is, therefore, critical in this respect. In addition, co-ordination

between member states' activities at European Union level and government representatives at national level will be important and the new Board will need a single contact point to liaise with the various Government Departments involved.

- Information Society Commission
  The major initiatives being taken by the Information Society Commission in relation to the successful exploitation of the new technologies are, the Group feel, inseparably linked to ongoing measures to combat their illegal and harmful use. The positive planning of this country's successful use of the Internet must proceed in step with measures to create a safe Internet environment. Both approaches need to be co-ordinated and the Group considers that representation on the Advisory Board by an Information Society Commission representative is an effective way of addressing the issue of balance.

- Education and Child Protection
  The European Commission Recommendation on the Protection of Minors and Human Dignity in the Audio-visual and Information Services[11] states:

  > *The voluntary nature of self-regulation means that the acceptance and effectiveness of a national self-regulation framework depends on the extent to which the parties concerned actively co-operate in its definition, application and evaluation.*

  The inclusion of those who have been the initial focus of attention of the Group is, accordingly, crucial and we feel that the education and child protection sectors should be represented.

- Legal
  There is also a requirement to include a member with legal experience to provide advice on the legal issues which will inevitably arise in the course of the Board's deliberations. This is without prejudice to the requirement from time to time for specialist independent legal advice on specific legal matters which may arise.

- Complaints Body Director
  One of the primary functions of the Advisory Board would be to ensure that the hotline is functioning effectively and is given the support necessary for carrying out its duties. While the hotline will operate within particular guidelines, the Group recommends that its Director should be a member of the Advisory Board. As a member of the Board, he or she should seek the advice, and where appropriate, decisions from the Board in relation to (a) issues and cases which are exemptions to general guidelines (b) general policy matters relating to the development and maintenance of the new self-regulation framework and (c) any other related matter which the Director considers appropriate.

- Temporary Members
  Provision should also be made for the co-option of temporary members onto the Board who, in the opinion of the Board, have a significant contribution to make on specific issues. Examples of such temporary membership would include specialists from industry and the public sector, including experts from other jurisdictions. For example, in view of the rapid convergence of broadcasting services and on-line services generally, an expert in the area of media regulation might be co-opted onto the Board at the appropriate time.

[11] The Green Paper on the Protection of Minors and Human Dignity in Audio-visual and Information Services. European Commission Document (96) 483, 16 October 1996.

5.4.3 Functions of the Board

We recommend that the Board's functions should include the following:

- The setting up of the hotline in accordance with funding arrangements to be agreed between Government and service providers.
- The establishment of viable and transparent procedures for processing complaints.
- The promotion and monitoring of all measures required to implement an effective system of self-regulation for the safe use of the Internet.
- Co-ordination between the various players in the context of establishing a framework for self-regulation.
- Consideration and decisions on all matters submitted by the Director of the hotline.
- Contribution to the development of standards and procedures for the hotline.
- Agreement and decision on how particular issues and problems should be addressed including identification of the specific steps to be taken and the particular parties who should take those steps.
- Liaison with relevant and comparable international bodies particularly within the context of the initiatives currently taking place at European Union level.
- Identification and prioritisation of appropriate research into Internet downside issues.
- Review on a regular basis, of the composition, structure and effectiveness of the Board itself and the Complaints Agency in the context of emerging national and international developments.
- Monitoring of progress on all aspects of self-regulation and reporting to Government and industry via an Annual Report.

5.4.4 Need for flexibility

Flexibility of operation will be critical

The Advisory Board will be working in a rapidly-changing environment and must be capable of adapting to changing circumstances. We have been acutely aware of the significant developments which have taken place both nationally and internationally, even during the period of our own deliberations. Flexibility of operation will be critical and such flexibility will only be achieved by a real commitment to the partnership concept of the self-regulating model. While the Group felt the necessity to set down the outline composition and structure of these new bodies, they should have the freedom and capacity to adapt to new circumstances while at the same time maintaining the stability which goes with sound administrative practice coupled with documented guidelines and procedures.

5.5 Overview of strategies

A summary of the various proposed strategies based on jurisdiction and material type is shown in the matrix below:

	ILLEGAL MATERIAL	HARMFUL MATERIAL
Material <u>within</u> Jurisdiction	Examples • child pornography on Newsgroups • illegal material on Irish websites Strategies • potentially illegal material reported to hotline • hotline asks SP to remove material • Garda informed if SP fail to remove • if posted in Ireland, Gardaí may contact author • hotline and Board to design and document procedures for complaints handling • hotline and Board to develop common strategies for "difficult" blocking issues • awareness campaigns at national and sectoral level (including service providers) Service involved • Newsgroups/Bulletin Boards • WWW	Examples • sexually explicit material on newsgroups • incitement to hatred material on Irish Website Strategies • acceptable usage conditions • service provider codes of practice • support by hotline and Advisory Board of national and international rating systems development • creation of "white sites" for particular sectors • development of software products by Irish industry to enhance internet safety • Advisory Board to co-ordinate • awareness campaigns at national and sectoral level (including service providers) Services involved • newsgroups • WWW • chat

	ILLEGAL MATERIAL	HARMFUL MATERIAL
Material <u>outside</u> Jurisdiction	Examples • child pornography on Japanese websites - accessible from Ireland • illegal material on newsgroups accessed from Ireland but through the local service provider • legal Irish sites which have links to illegal foreign sites Strategies • participation in EU initiatives by hotline and Board • hotline to liaise with appropriate hotlines abroad • liaise with Gardaí re international police co-operation measures • awareness campaigns at national and sectoral level (including service providers) Services involved • WWW • newsgroups and bulletin boards not held locally • chat channels	Examples • racial discrimination items on American websites Strategies • international co-operation of hotlines and advisory groups, • participation in EU initiatives by relevant parties • awareness campaigns at national and sectoral level (including service providers) Service involved • WWW • newsgroups • chat channels

5.6 AWARENESS OF THE ISSUES

5.6.1 Individual responsibility

Awareness measures are a vital complementary tool

The final strategic measure recommended by the Group focuses on the need for appropriate awareness programmes so that everyone involved in using the Internet can play their part in addressing its illegal and harmful use. We see this as a vital complementary tool that is an essential part of the overall response. Knowledge in this instance is, in fact, power. As is evident from the Report so far, there are areas where technical and structural responses of themselves are not the complete answer. In the final analysis, society must take a significant amount of responsibility at the level of the individual. The continued development of international rating systems and their associated filtering tools may ultimately place content choice in the hands of the user. Given responsible and informative parents and educators, this will provide a real, significant and workable opportunity to create and maintain a safe Internet environment.

5.6.2 Integration with Information Society Commission initiatives

The Group is conscious and appreciative of the emphasis placed by the First Report of Ireland's Information Society Commission on the need for awareness of the new information technologies.

This Report identified a range of awareness campaigns and we feel that these campaigns should be complemented by material which allows all users to understand and respond to the challenges posed by the downside of the Internet. Separate awareness campaigns will, we believe, be less likely to be successful than if an integrated approach is adopted. We recommend, therefore, that wherever feasible, any national or sectoral information society awareness campaign proposed under the auspices of the Commission, include a dimension which addresses the potential for illegal and harmful use of the Internet.

5.6.3 Specific initiatives

At a micro level, the Group believes that a wide range of sectoral awareness initiatives is appropriate and should be undertaken. Specifically we recommend:

- Service providers should, as part of their ongoing and routine contact with their clients, use all means at their disposal, including the Internet itself, to educate clients on the safe use of the Internet.

- The new hotline and the Advisory Board should proactively stimulate and encourage the development of awareness initiatives and contribute to the development of appropriate material for inclusion in awareness campaigns.

- Specific groups such as parents and teachers should be targeted. Information leaflets such as those used by the NCH Action for Children in the United Kingdom, were noted by the Group as being particularly useful and appropriate.

- Modules on Internet safety should be incorporated into the curriculum of teachers, care workers, Gardaí, Customs officers and any other agencies who come in contact with issues relating to the downside of the Internet.

Initiatives for schools

More specifically within the schools environment, the following particular initiatives are recommended:

- In-career training modules on Internet issues
  The Group recognised the importance of imparting a significant level of knowledge on Internet issues to teachers who will supervise Internet sessions and projects in the classroom. If students are aware that teachers have sufficient expertise to be aware of the possibilities for misuse, the risks of undesirable activity will be minimised.

- Publication of Guidelines
  The Department of Education and Science should undertake the publication of a set of guidelines for those involved in the use of the Internet in the schools context. Such guidelines should address the main areas of concern to teachers and parents and incorporate elements of best practice in other jurisdictions.

- Integration of Internet Ethics into the Curriculum
  The importance of availing of opportunities to impress upon students the correct ethical behaviour in relation to Internet access cannot be underestimated. A fuller understanding of the need to protect the integrity of all those involved in the use of the medium is considered an essential element in an effective education strategy.

- Information Sessions for Parents
  The Department of Education and Science should consider the feasibility of acquiring parental sign-off to permit student Internet access in consultation with parents representatives. This would place a duty on the parent/guardian to be aware of the

possibilities in relation to the use by students of the Internet and this policy could be supported by the staging of open information sessions for parents. Such sessions could provide a balanced view of the dangers and benefits of Internet access, with appropriately strong emphasis on the positives aspect of the technology. This approach would also be beneficial in the context of parental concerns about children who may have Internet access at home, where the technology and its implications may not be fully understood.

- Schools Code of Conduct
  The Department of Education and Science, should devise a code of conduct for the use of information and communication technologies at school level, covering all aspects of usage, rights, access control, responsibilities, ethics and good practice for students and educators. To be effective, the code would have to be formally signed off by all participants and penalties for non-observance clearly specified.

The Group was also conscious that there are very many groups and organisations involved in the interface between technology and society. They would be particularly well-positioned to assist in getting across messages about the safe use of the Internet. Individual sectoral initiatives in this area should be encouraged.

5.7 FUNDING ISSUES

5.7.1 Independent funding

Funding should be provided by the SP's

As a matter of principle, funding for the establishment of hotlines should be provided by the Service Provider Industry itself as is the case in a number of countries such as the United Kingdom, Holland and Germany. Ownership and control of the self-regulation process should be in the hands of the industry and industry funding is a useful mechanism for ensuring that this will happen.

5.7.2 Benefits to industry

Tangible benefits do accrue to the industry from the establishment of a hotline and the introduction of an overall self-regulating framework. It assists the industry to help promote a safe Internet environment for their clients and enhances their corporate image as being responsible businesses. It also provides a forum through which common problems can be addressed. In relation to illegal material on the Internet, it offers a pragmatic and workable framework within which positive co-operation with the Gardaí is facilitated.

5.7.3 Other alternatives

Other funding arrangements do, however, exist. In Belgium and Austria, there is a strong law enforcement dimension to the funding arrangements for hotlines and in Norway, joint arrangements exist between child organisations and the Ombudsman for Children.

5.7.4 Ireland - a special case

Self-funding in the Irish context does, however, give rise to some problems and a number of factors exist which influenced the Group's recommendations in this regard. The Service Provider market in Ireland is still relatively under-developed and is undergoing rapid change in terms of the structure of its ownership. There is a small number of Service Providers of any significant size and two of these are currently under the ownership of semi-State Companies. The market is, however, a developing one and it is not possible to forecast a development profile of the service provider industry with any degree of accuracy.

Taking into consideration an across-the-board profile of the Service Provider industry in Ireland, the Group is concerned that the industry, because of market size and stage of development, is not currently in a position to provide the funding which will be needed immediately to establish the proposed hotline. In view of this assessment and of the need to establish the hotline as an immediate priority, the Group recommends that funding support be provided by Government, at least in the short term, pending the establishment and consolidation of the industry on a more substantial footing.

Government should provide funding support in the short term

It is recommended, therefore, that the funding of the new hotline be shared by Government and Industry. The Group recommends that immediate discussions take place with industry with a view to agreeing the detailed funding arrangements. However, whatever arrangements are agreed, they should reflect a reduction of the Government contribution in line with the growth and development of the industry.

5.7.5 Secretariat arrangements

In view of the critical and immediate role to be played by the Advisory Board in establishing the hotline, the Group recommends that its secretariat should also be provided by Government. Apart from funding requirements arising from its ongoing remit in relation to the hotline, (legal advice, research etc.) it is anticipated that costs will arise in the context of the Board's need to actively liaise with international developments, particularly in the European Union.

5.7.6 EU funding opportunities

As part of their initiatives to encourage self-regulation, the European Union have announced special projects which they are prepared to part-fund for industry. Fortunately, they cover almost all the areas covered by the recommendations in this Report. These projects are complementary to the other areas of European Union initiatives and are considered to be a means of implementing a European approach to the safe use of the Internet based on industry self-regulation, filtering and rating systems and awareness programmes. A call for proposals is being made for part-funding of projects related to; the establishment of national hotlines; work on content filtering and rating systems; and preparatory awareness actions linked to safe use of the Internet. The Group recommends that the Industry actively and immediately pursue such funding opportunities so as to facilitate a tripartite approach to funding, at least in the short term.

EU funding should be taken up

5.8 OTHER ISSUES

As already outlined, this first Report of the Working Group on the Illegal and Harmful Use of the Internet reflects the priority given to the issue of child pornography and the need to establish a structural framework within which immediate progress can be made. There are still a wide range of issues yet to be considered in the context of examining the illegal and harmful use of the Internet.

5.8.1 "Internet-proofing" of new legislation

For example, our consideration of the legal aspects of the Internet were, in the main, focused on providing the best response possible to emerging proposals on the Child Pornography Bill. Many further important legal issues need to be examined. The Information Society Commission have already identified areas of legislation which will impact on the illegal use of the Internet, particularly in the area of copyright and intellectual property. While the Group examined a small number of legal provisions as discussed in Section 3.3, we are not yet in a position to make specific legal recommendations. Work currently being undertaken in a European Union context will be very relevant in this regard.

All new legislation to be checked for "Internet" compatibility

Nevertheless, on a more general front, we recommend that any review of existing legislation take into account the implications for illegal use of the Internet, having regard in particular to the nature of the technology and the medium used. As a practical measure, we further recommend that all new legislation be formally checked for "Internet compatibility" before being submitted to Government for approval.

5.8.2 The encryption issue

In discussing the 1993 Interception Act, it was felt that the principle had been established that in limited circumstances and subject to appropriate safeguards, the appropriate State Agency should have the power to intercept telecommunications messages. This led on to a consideration of the issue where encryption could make interception impossible. The Group is aware that this matter is being examined both at a national and European Union level.

Improvements in encryption pose challenges for Internet downside issues

A resolution of this issue is needed which reconciles the need for privacy protection and commercial integrity on the one hand with the requirements of law enforcement agencies on the other. The increasing efficiency and the wider availability of encryption products cause a major challenge to successful strategies for dealing with the illegal and harmful use of the Internet. Given the emerging international commitment to both commercial exploitation of the Internet and the protection of our young people, it would appear that balance in this difficult issue can only be resolved at international level.

At this point in time, the Group recognises that it can only flag the issue as one of major importance for the practical implication of whatever national legislation is enacted to address the illegal use of the Internet within its jurisdiction. There are considerable dangers in having laws which, for whatever reasons, are incapable of being policed because the required evidence is not accessible.

5.8.3 Specialist training

Enforcing the law in relation to the Internet will require specialist expertise in a wide range of technical and evidential areas. In this regard, the Group notes that initiatives in the area of specialist training for An Garda Siochana have already commenced. We recommend that these initiatives be pursued as a matter of urgency and that training in this specialist area be extended to the wider areas of law enforcement including members of the judiciary.

5.8.4 Other parallel initiatives

There is no reason why individual initiatives could not address particular protection issues already identified in the Report. For example, the Group is aware that some ISPs are planning the introduction of family-oriented subscription services, using dedicated servers to control access levels. Controlled content may be locally generated or provided through the replication of appropriate entertainment or educational materials from international sources. The latter initiative reflects the concept of "white site development", where sub-sets of the Internet are specially screened for a particular target group such as children.

Other content control initiatives under consideration relate to the control of e-mail through parental involvement. For example, copies of all e-mail messages sent and received can be copied to the parent's mailbox. Managed "live" events incorporating IRC (Internet Relay Chat) can be organised on a scheduled basis and moderated by ISP staff.

Selling safety is good business

Initiatives like the above could be pursued in parallel with developments in rating systems. Indeed, as already mentioned, commercial considerations alone will inevitably drive many similar projects aimed at providing a safe environment for Internet users. The Group is of the view that "selling" safety is good business and that part of the overall objective of the self-regulatory environment will be to encourage co-operation in the development of such projects among the service providers.

5.9 WORKING GROUP - NEXT STEPS

The terms of reference given to the Group in 1997 were broad enough to allow it to continue examining other issues relating to the illegal and harmful use of the Internet. As pointed out in our Report, however, we are working in a rapidly evolving environment and we ourselves must adjust our work focus to new national and international developments. Against this background, the first task of the Group will be to re-examine its composition and prepare a new set of priority issues for our next Report.

Appendices

APPENDIX 1

WORKING GROUP ON THE ILLEGAL AND HARMFUL USE OF THE INTERNET

Main Group Membership

John Haskins	Chairperson, Department of Justice, Equality and Law Reform
Brenda Boylan[12]	Department of An Taoiseach
Cormac Callanan	Internet Service Providers Association of Ireland
Audrey Conlon	Deputy Film Censor
John Deady	Department of Foreign Affairs
Jim Duffy	Department of Finance
Jim Grant	Office of the Revenue Commissioners
Colm Grealy[13]	Ireland on Line
Mark Henry	Policy Watch
Brian Millane	Department of Arts, Heritage, Gaeltacht and the Islands
Patrick Mooney	Office of the Attorney General
Tom O'Reilly	Department of Enterprise, Trade and Employment
Noel O'Sullivan	Chief Superintendent, An Garda Siochana
Christy Philpott	Department of Education and Science
Maura Quinn	UNICEF
Dermot Ryan	Department of Health and Children
Prof. Kevin Ryan	University of Limerick
Prof. Max Taylor	University College Cork
Fintan Towey	Department of Public Enterprise

Replacements, substitutes and specialist contributors:

Eddie Branigan	Department of Foreign Affairs
Richard Fennessy	Department of Justice, Equality and Law Reform
Michael Gaffey	Department of Foreign Affairs
Paul Hickey	Department of Justice, Equality and Law Reform
Dermot McCarthy	Department of Health and Children
Paul Murray	Department of Justice, Equality and Law Reform
Kay Nolan	UNICEF
Éanna Ó'Conghaile	Department of Public Enterprise
Rachel O'Connell	University College Cork
Michael Perkins	Department of Health and Children
Anne Varley	Department of Justice, Equality and Law Reform
Noel White	Department of Foreign Affairs

Secretariat

Niall Cullen	Department of Justice, Equality and Law Reform

[12] Ms Boylan transferred to the Secretariat of the Information Society Commission during 1997.

[13] Mr Grealy initially represented the service providers interests before the ISPAI was formed.

APPENDIX 1

SUBGROUP MEMBERSHIP

Legal Subgroup

Patrick Mooney (Chair)
Cormac Callanan
Richard Fennessy
Jim Grant
Paul Murray
Fintan Towey

Service Provider Subgroup

Jim Duffy (Chair)
Cormac Callanan
Audrey Conlon
Colm Grealy
Mark Henry

International Subgroup

Brenda Boylan (Chair)
John Deady
Michael Gaffey
Brian Millane
Kay Nolan
Prof. Kevin Ryan
Anne Varley
Noel White

Child Issues Subgroup

Christy Philpott (Chair)
Chief Superintendent Noel O'Sullivan
Michael Perkins
Maura Quinn
Dermot Ryan
Prof. Max Taylor

APPENDIX 2

SUBMISSIONS TO THE WORKING GROUP

Written Submissions:

Advertising Standards Authority for Ireland, 35/39 Shelbourne Rd, Dublin 4.

Association of Secondary Teachers Ireland (A.S.T.I.), Winetavern St, Dublin 8.

Barnardos, Christchurch Square, Dublin 8.

Cable Communications Association of Ireland, 70 Capel St, Dublin 1.

Mr. Alan Carr, 13 Walsh's Terrace, Woodquay, Galway.

Catholic Primary School Managers Association, Veritas House, 7/8 Lower Abbey St, Dublin 1.

Central Bank of Ireland, Dame St, Dublin 2

Childrens Rights Alliance, 4 Christchurch Square, Dublin 8.

Cork County Council, County Hall, Cork.

Cyberia Cafe, Arthouse Multimedia Centre, Curved St, Temple Bar, Dublin 2.

Data Protection Commissioner, Block 4, Irish Life Centre, Talbot St, Dublin 1.

Electronic Frontier Ireland, 56 Westgate, Saint Augustine St, Dublin 8.

Irish Association of Social Workers, 114-116 Pearse St, Dublin 2.

IBEC, Confederation House, 84/86 Lower Baggot St, Dublin 2.

Irish Music Rights Organisation (IMRO), Pembroke Row, Lr. Baggot St, Dublin 2

Irish National Teachers Organisation (INTO), 35 Parnell Square, Dublin 1.

Irish Service Providers Association Document " Internet Players and their Respective Roles" (copies available on request, c/o 425 Richmond Court, Milltown, Dublin 6).

Ms. Muireann O'Briain SC, 17 Charleville Rd, Rathmines, Dublin 6.

National Lottery, Lower Abbey St, Dublin 1.

Parents Association of Community and Comprehensive Schools, Avondale, John St, Ardee, Co. Louth.

Regtel, 32 Nassau St, Dublin 2.

Teachers Union of Ireland (TUI), 73 Orwell Rd, Rathgar, Dublin 6.

UCD Audio Visual Centre, Belfield, Dublin 4

APPENDIX 2

Submissions by e-mail:[14]

America Online Inc/AOL Bertelsmann Online UK, 20 Fulham Broadway, London SW61

Mr. Fergal Byrne, Adnet Ltd, 23 St. Stephens Green, Dublin 2.

Mr. Mark Dowling, 2 Malboro Mews, Wellington Road, Cork.

Mr. Padraig Finnerty, 1 Broadway Drive, Blanchardstown Dublin 15.

Global Internet Liberty Campaign c/o Mr.Yaman Akdeniz, Centre for Criminal Justice Studies, University of Leeds, UK.

Mr. Martin Hayes, Director, Computer Centre, University College Cork.

Mr. Matthew Hogan, Attorney at Law, 2320 Oakland Blvd, Fort Worth, Texas, USA.

Dr. Roy Johnson, Techne Associates, P.O.Box 1881, Rathmines, Dublin 6.

Mr. Rory O'Farrell, Tinode, Blessington, Co. Wicklow.

Mr. John Plunkett, Connect Ireland Communications Ltd, 20 Mark St, Dublin 2.

Mr. Damian Ryan, Publisher "Dot. ie" Internet Magazine, 6 Camden Place, Dublin 2.

Mr. Stephen Glanville, Barrister at Law, 7 Tara Grove, Wellpark, Galway.

Oral Submissions

AOL Bertelsmann Online, 20 Fulham Broadway, London, SW 61 AH, England.

Data Protection Commissioner, Block 4, Irish Life Centre, Talbot St, Dublin 1.

Focus on Children, 13 Gardiner Place, Dublin 1.

National Parents Council, Primary, 16-20 Cumberland Street South, Dublin 2.

National Womens Council of Ireland, 16-20 Cumberland Street South, Dublin 2.

R.T.E.. Donnybrook, Dublin 4.

[14] The Group also wishes to acknowledge a number of unsigned e-mail submissions submitted for its consideration.

APPENDIX 3

INTERNET SERVICE PROVIDERS ASSOCIATION OF IRELAND (ISPAI)

Membership list

Club Internet

4 Lower Mount Street
Dublin 2

Esat Net

4 Westland Square
Dublin 2

Indigo

61-62 Fitzwilliam Lane
Dublin 2

Ireland On Line/Post Gem

Alexandra House
Earlsfort Terrace
Dublin 2

Telecom Internet/Eirtrade

Merrion House
Merrion Road
Dublin 4

APPENDIX 4

GLOSSARY OF INTERNET TERMS

Browser
A software tool used to look at Web pages on the Internet.

Chat
A way of conducting instantaneous typed “conversation” through the Internet.

Chat channels
These are virtual “discussion rooms” which typically focus on specific subject areas.

Discussion Groups
These include newsgroups and mailing lists and represent areas of the Internet where discussion takes place on a wide variety of topics.

Domain name
Every computer when connected to the Internet has a unique number (an IP address). To help users in finding particular computers, most computers connected to the Internet have a more meaningful language-based name called a “domain name”. For example, most of the Irish Government computers on the Internet have irl.gov.ie as their domain name.

Encryption
The process of encryption “scrambles” electronic material into a form which can only be read or “unscrambled” using a code or key.

Extranet
A network which uses Internet technology and which allows organisations to communicate with selected others involved in its business. For example, a factory might use an extranet to communicate with its suppliers and customers.

File Transfer Protocol (FTP)
A means of sending, storing and receiving files on the Internet.

Filtering software
A software tool used to detect a rating or a classification applied to the contents of Internet material in order to detect the use of words or terms considered to be harmful.

Home page
The first page or “starting” page of a particular entry in the WWW. It usually provides links to other more detailed pages.

Information superhighway
A general name given to the sophisticated telecommunications infrastructure of which the Internet is a part.

Internet
A “network of networks” of computers.

Intranet
A private version of the Internet that lets people within an organisation exchange data using Internet technology.

Mailing lists

A form of discussion group in which participation is by simple electronic mail. Contributions are made to a particular e-mail address which then acts as a post box for distribution to a predefined list of addresses. Essentially, the particular e-mail address re-mails all incoming mail to a list of subscribers to the mailing list

Messaging protocols

Rules used by the Internet to send different kinds of messages through its networks.

Mirror sites

These are web sites which hold copies of information held at other sites. Copies are sometimes made and relocated for very legitimate reasons. On the other hand, copies are sometimes made and relocated in order to avoid detection.

Network

A group of connected computers; also used to describe the telecommunications system.

Newsgroups

A form of discussion group where contributions are organised by subject matter.

News server

The name given to any computer on the Internet which stores newsgroups.

On-line

A computer is on-line when it is connected to a network or another computer.

Packet-switched services

A method of electronic transmission which divides information into discrete “packets” during transmission and then reassembles the packets on delivery at final destination.

Peer to peer

This occurs when users’ computers are connected directly to each other over the Internet.

Rating systems/labels

Internet content can be rated or classified in terms of the kinds of material it contains. There are standard systems to help in this rating which can be used by content providers to allow users to decide what level of nudity, violence etc. is acceptable to them.

Search engines

Software which allows Internet users to access material in the WWW simply by typing in specific words or phrases.

Server

A computer that provides service to Internet users. It can make programs, web sites, files or other material available to such users.

URL

The Uniform Resource Locator is the name give to the unique address where particular files or documents are stored on the World Wide Web.

APPENDIX 4

Usenet

The collective name given to newsgroup services on the Internet.

White sites

Specially selected subsets of the Internet extracted by service providers which are usually geared towards a particular target group such as children.

Web page

A “screenful “ of material on the World Wide Web - somewhat akin to a page of a book.

Web sites

A collection of Web pages usually focused on a particular topic or devoted to a particular organisation.

World Wide Web (WWW)

The complete library of text, graphic and audio material available through the use of special software called a browser.

APPENDIX 5

COURT CASES

Some recent court cases as examples of activities in the child pornography area:

Case 1

In December, 1996, a member of the clergy in Durham, UK, was convicted of, among other charges (including indecent assaults on two boys), distributing indecent photographs and possessing them with intent to distribute them. His home computer systems had almost 9,000 images of child pornography, adult pornography and related drawings, mainly obtained through use of the Internet. He had connections to the Internet from four different ISPs and used encryption software. Evidence presented in court showed that he used e-mail to correspond extensively and exchange material with nine other members of a paedophile ring in many parts of the world. One of his victims wanted to relocate as he feared his name and address had been circulated on the Internet.

The case was unique in that it was the first in the UK to establish a direct link between child abuse and the Internet and it uncovered the largest known collection of illicit material gathered electronically. He was sentenced to six years.

Source: The Times (London), 13 November, 1996

Case 2

In November, 1996, a general practitioner from Wiltshire, UK was convicted, having been found to be in possession of images of children in indecent poses stored on his home computer. Evidence presented in court showed him to be an extensive user of IRC. He was sentenced to community service.

Source: The Telegraph, 7 December, 1996

Case 3

Operation Starburst
The British police participated in Operation Starburst, in July 1995, an international investigation of a paedophile ring who used the Internet to distribute graphic pictures of child pornography. Nine British men were arrested as a result of the operation which involved other arrests in Europe, America, South Africa and the Far East. The operation identified 37 men worldwide. Detective Inspector David Davis, head of West Midlands Police Commercial Vice Squad stated that:
“The pictures ranged from nudity, through erotica to explicit sexual material involving children, one as young as three.”

Source: Akdeniz (1997)[15]

[15] Regulation of Child Pornography on the Internet, Cyber-Rights and Cyber-Liberties UK, 1997

Case 4

In early 1996, a former computer consultant was sentenced to three months' imprisonment at a Birmingham magistrates court. He also admitted to being in possession of indecent pictures of children and was the first person to be jailed in the UK for an offence concerning pornography and the Internet.

Source: The Telegraph, 5 January, 1996

Case 5

In October, 1993, police executed a search warrant at the Toronto home of 19-year-old man. They found stories and images depicting sex with children on his home computer, which was connected to the Internet. The man was arrested and charged as part of Project Front Door, a Metro Toronto police investigation into a variety of computer-related crimes. In 1995, the man - who used the alias "Recent Zephyr" on computer bulletin boards - became the first person in Canada convicted of distributing child pornography via computer.

Source: Skelton (1996)[16]

Case 6

Two men, one of whom worked in Birmingham University collected thousands of pictures in the University computer system of youngsters engaged in obscene acts. The material could be accessed through the Internet across the world. The University worker had built up an extensive library of explicit pornography called "The Archive", featuring children as young as three, on a computer at the University.

At their trial in 1996, they had argued that because the pictures were stored on a computer hard disc they could not be regarded as photographs and could not be covered by obscene publications legislation. The judge ruled that the computerised images could be legally regarded as photographs and the case set a legal precedent that a pornographic computer image was, in law, the same as a photograph.

The University worker was jailed for three years by the trial judge who said that what he had done could have incited sexual abuse of the innocent. He was informed that the sentence was intended to act as a deterrent to others considering using the computer information network to circulate pornography. The second man was also jailed for six months for providing the University employee with up to 30 pornographic pictures of children.

Source: Cyberia Magazine, August, 1996; Akdeniz (1997)

Case 7

A man from Belfast was fined £4000 for possession of child pornography in July 1997. The Police raided his home when it was discovered that a disk he left behind at a Belfast Internet cafe contained child pornography. The police found images of child pornography on diskettes and also on the hard disk of his computer. The man admitted getting the material from the Internet.

Source: Akdeniz (1997)[17]

[16] Child-less Pornography: Thought kiddie-porn always involved the direct abuse of children? Think again., id Magazine, 25 January, 1996

[17] Regulation of Child Pornography on the Internet, Cyber-Rights and Cyber-Liberties UK, 1997

APPENDIX 6

DESCRIPTION OF PICS[18] PLATFORM AND RASC[19] RATING SYSTEM

P.I.C.S. (PLATFORM FOR INTERNET CONTENT SELECTION)

PICS - A set of technical specifications for creating rating systems and filtering software for Internet content.
PICS was developed by the World Wide Web Consortium (located at MIT in the United States and INRIA in France), along with the support and participation of a large number of companies around the world.
PICS specifies how to create rating labels for Internet content.

Rating labels - Indicate specific aspects of content, such as offensiveness of language, explicitness of sex and the degree of violence.

Rating systems - The particular set of criteria used for creating labels. There are a number of such systems in the market. The RSAC system is described below.

Rating services - Determine the substance of the labels by setting the criteria. The labels can be applied by Web publishers themselves (“self-rating”) or by independent organisations (“third-party rating”).

Filtering software - Used to automatically read the labels and block content that does not fit the criteria specified by the Internet users themselves. (See Appendix 7 also)

The PICS platform allows a single Web site to have multiple labels applied by different rating systems. Parents can choose whether to block their children’s access to content that has no label at all, or to override the block after viewing the material. As the usage of the Internet and the awareness of filtering technology grows, parents will have a growing variety of rating services from which to choose, and will be able to select those which most closely reflect their own values

RSAC (THE RECREATIONAL SOFTWARE ADVISORY COUNCIL)

RSAC - An independent, non-profit organisation based in Washington, D.C, that empowers the public, especially parents, to make informed decisions about electronic media by means of an open, objective, content advisory system.

The RSAC system provides consumers with information about the level of sex, nudity, violence, offensive language (vulgar or hate-motivated) in software games and Web sites. To date, RSAC has been integrated into Microsoft’s browser, Internet Explorer, and MicroSystem’s Cyber Patrol Software. CompuServe (US and Europe) has also committed to rate all its content with the RSAC system.

Rating The Web - The aim in creating RSAC on the Internet was to provide a simple, yet effective rating system for web sites which both protected children and protected the rights of free speech of everyone who publishes on the World Wide Web.

[18] Based on PICS booklet “An Industry solution for the protection of children in the information society” 1997. Further information available from jmiller @w3.Org

[19] Based on information on RSAC website at http://www.rsac.org

APPENDIX 6

Parental Controls - RSAC designed a system based on the tried and tested content advisory system used for computer games and one which could be simply understood and set by parents at either the browser level (e.g. Microsoft's Internet Explorer) or blocking device (e.g.. CyberPatrol).

Setting The Levels - The table below shows the four categories of the RSAC system with the five levels and their descriptors. It is these levels that parents and other interested individuals will set at their browser or blocking device.

Levels	Violence Rating Descriptor	Nudity Rating Descriptor	Sex Rating Descriptor	Language Rating Descriptor
4	Rape or wanton, gratuitous violence	Frontal nudity (qualifying as provocative display)	Explicit sexual acts or sex crimes	Crude, vulgar language or extreme hate speech
3	Aggressive violence or death to humans	Frontal nudity	Non-explicit sexual acts	Strong language or hate speech
2	Destruction of realistic objects	Partial nudity	Clothed sexual touching	Moderate expletives or profanity
1	Injury to human being	Revealing attire	Passionate kissing	Mild expletives
0	None of the above or sports related	None of the above	None of the above or innocent kissing/ romance	None of the above

APPENDIX 7

FILTERING PRODUCTS

Introduction

An important weapon in the armoury of those seeking to prevent access by minors or vulnerable individuals to illegal or harmful material on the Internet is that of filtering. A range of specially written commercial software is available for installation on PCs or Local Area Networks (LANs) to screen out objectionable sites and material.

PC-based Filtering Software

Filtering software works in conjunction with the Web Browser software installed in the PC. Typical popular products include Net Nanny, Cybersitter, Cyber Patrol and Rated PG. Most filtering products work primarily by blocking access to objectionable sites, the URLs for which they store in a hidden list. Some products permit a parent to customise this list, either by adding the URLs of additional offensive sites or by deleting references to sites previously blocked.

The products of certain vendors can be supplemented with a service whereby updated lists can be provided on an ongoing basis for direct installation by the subscriber. It is important that products offering this functionality should also block the IP address corresponding to the URL, so that the blocking capability of the software cannot be subverted through entering the IP address alone.

An alternative approach used in some products is that of limiting access only to sites deemed appropriate for children. This technique is referred to as whitelisting. Other filters simply check URLs, entries in Internet searches and Web pages for occurrences of inappropriate words, replacing them with a series of Xs.

The shortcoming with a list-based approach is that it can never be considered complete because thousands of new sites go on-line each day. Therefore, having the additional functionality to search for and block unsuitable words is an important feature of the software. However, a potential difficulty with this approach is that sites which have merit, and to which access would be appropriate, could be blocked, due to the lack of sophistication in the blocking method. Products which can overcome this limitation, through recognising the context of the key words, have evidently greater merit than those which cannot.

A useful feature which some products offer is that of controlling the time of day and length of time for which Internet sessions can be conducted. This permits parents to restrict sessions only to those times when supervision is available.

Software which prevents the disclosing of personal information provides another layer of protection for minors on the internet, as they may not always be able to judge the intentions of seemingly innocent queries from unidentifiable correspondents using Email or chat rooms.

The features overleaf can be assessed when considering the appropriateness of these software tools.

FEATURE DESCRIPTION

Blocking on Key Words or Phrases:

URLs, Newsgroups, Net searches and Chatrooms are checked against a list for offensive material and access is granted or denied on that basis.

Exclusive Site Lists (Blacklisting):

Access to an extensive, often customisable, list of sites is blocked. Generally the vendor generates and updates a list of sites which have been found to be unacceptable.

Inclusive Site Lists (Whitelisting):

A subset of the internet is identified as acceptable for access and the software blocks entry to sites not explicitly included in the control list.

Controlling time and length of access to the internet

To facilitate control over children's access to the internet, some software products can be configured to allow access to the Internet for short periods and only at specified times of the day.

Automatic Monitoring and Logging of Internet Activity

A log of all activity, including sites visited, is created. This log cannot be accessed by the child, and is protected by password from deletion/modification.

Restricting the disclosure of Personal Information

Software is available which will prevent children from divulging personal information. That is, the minor is restricted from disclosing a name and address, using credit card numbers or volunteering other inappropriate information.

APPENDIX 8

GREEN PAPER GUIDELINES

(from Proposal for a European Council Recommendation concerning the protection of minors and human dignity in audiovisual and information services)

INDICATIVE GUIDELINES FOR THE IMPLEMENTATION, AT NATIONAL LEVEL, OF A SELF-REGULATION FRAMEWORK FOR THE PROTECTION OF MINORS AND HUMAN DIGNITY IN AUDIO VISUAL AND ON-LINE INFORMATION SERVICES

Objective

The purpose of these guidelines is to ensure broad consistency, at European Union level, in the development, by the businesses and other parties concerned, of national self regulation frameworks for the protection of minors and human dignity in the audiovisual and on-line information services industry. The services covered by these guidelines are those provided at a distance, by electronic means. They do not include broadcasting services covered by the "Television Without Frontiers" Directive or radio broadcasting. The contents concerned are those which are clearly intended for the public, rather than private correspondence. This consistency will enhance the effectiveness of the self-regulation process and provide a basis for the necessary transnational cooperation between the parties concerned.

While taking into account the voluntary nature of the self-regulation process - the primary purpose of which is to supplement existing legislation - and respecting the differences in approach and varying sensitivities in the Member States of the European Union, this Annex recommends indicative Guidelines on four key components of a national self-regulation framework.

- consultation and representativeness of the parties concerned,
- code(s) of conduct,
- national bodies facilitating cooperation at European Union level,
- national evaluation of self-regulation frameworks.

I. CONSULTATION AND REPRESENTATIVENESS OF THE PARTIES CONCERNED

The objective is to ensure that the definition, implementation and evaluation of a national self-regulation framework benefits from the full participation of the parties concerned, such as the public authorities, the users, consumers and the businesses which are directly or indirectly involved in the audiovisual and on-line information services industry. The respective responsibilities and functions of the parties concerned, both public and private should be set out clearly.

The voluntary nature of self-regulation means that the acceptance and effectiveness of a national self-regulation framework depends on the extent to which the parties concerned actively co-operate in its definition, application and evaluation.

All the parties concerned should also help with longer-term tasks such as the development of common tools or concepts (for example, on labelling of content) or the planning of ancillary measures (for example, on information, awareness and education).

2. CODE(S) OF CONDUCT

2.1 General

The objective is the production, within the national self-regulation framework, of basic rules which are strictly proportionate to the aims pursued; these rules should be incorporated into a code (or codes) of conduct covering at least the categories set out at 2.2 below, to be adopted and implemented voluntarily by the operators (i.e. primarily the businesses) concerned.

In drawing up these rules, the following should be taken into account:

- the diversity of services and functions performed by the various categories of operator (providers of network, access, service, content etc.);

- the diversity of environments and applications in on-line services (open and closed networks, applications of varying levels of interactivity).

In view of the above, operator may need one or more codes of conduct.

Given such diversity, the proportionality of the rules drawn up should be assessed in the light of:

- the principles of freedom of expression, protection of privacy and free movement of services,

- the principle of technical and economic feasibility, given that the overall objective is to develop the information society in Europe.

2.2 The content of the code(s) of conduct

The code (or codes) of conduct should cover the following:

2.2.1. Protection of minors

Objective

To enable minors to make responsible use of on-line services and to avoid them gaining access, without the consent of their parents or teachers, to legal content which may impair their physical, mental or moral development. Besides co-ordinated measures to educate minors and to improve their awareness, this should cover the establishment of certain standards in the following fields:

a) information to users

Objective

Within the framework of encouraging responsible use of networks, on-line service providers should inform users where possible, of any risks from the content of on-line services and of such appropriate means of protection as are available.

The codes of conduct should address, for example, the issue of basic rules on the nature of the information to be made available to users, its timing and the form in which it is communicated. The most appropriate occasions should be chosen to communicate the information (sale of technical equipment, conclusion of contracts with user, web sites etc.).

b) presentation of legal contents which may harm minors

Objective

Where possible, legal content which may harm minors or affect their physical, mental or moral development should be presented in such a way as to provide users with basic information on its potentially harmful effect on minors.

The codes of conduct should therefore address, for example, the issue of basic rules for the businesses providing on-line services concerned and for users and suppliers of content; the rules should set out the conditions under which the supply and distribution of content likely to harm minors should be subject, where possible, to protection measures such as:

- a warning page, visual signal or sound signal,
- descriptive labelling and/or classification of contents,
- systems to check the age of users.

Priority should be given, in this regard, to protection systems applied at the presentation stage to legal content which is clearly likely to be harmful to minors, such as pornography or violence.

c) support for parental control

Objective

Where possible, parents, teachers and. others exercising control in this area should be assisted by easy-to-use and flexible tools in order to enable, without the former's educational choices being compromised, minors under their charge to have access to services, even when unsupervised.

The codes of conduct should address, for example the issue of basic rules on the conditions under which, wherever possible, additional tools or services are supplied to users to facilitate parental control, including:

- filter software installed and activated by the user;
- filter options activated, at the end-user's request by service operators at a higher level (for example, limiting access to pre-defined sites or offering general access to services).

d) handling of complaints (“hotlines”)

Objective

To promote the well-organised and effective management of complaints about content which does not comply with the rules on the protection of minors and/or violates the code of conduct.

The codes of conduct should address, for example, the issue of basic rules on the management of complaints and encourage operators to provide the management tools and structures needed so that complaints can be sent and received without difficulties (telephone, e-mail, fax) and to introduce procedures for dealing with complaints (informing content providers, exchanging information between operators, responding to complaints etc.).

2.2.2. Protection of human dignity

Objective

To support effective measures in the fight against illegal content offensive to human dignity.

a) information for users

Objective

Where possible, users should be clearly informed of the risks inherent in the use of on-line services as content providers so as to encourage legal and responsible use of networks.

Codes of conduct should address, for example, the issue of basic rules on the nature of information to be made available, it's timing and the form in which it is to be communicated.

b) handling of complaints ("hotlines")

Objective

To promote the effective handling of complaints about illegal content offensive to human dignity circulating in audiovisual and on-line services, in accordance with the respective responsibilities and functions of the parties concerned so as to reduce illegal content and misuse of the networks.

The codes of conduct should address, for example, the issue of basic rules on the management of complaints and encourage operators to provide the management tools and structures needed so that complaints can be sent and received without difficulties (telephone, e-mail, fax) and to introduce procedures for dealing with complaints (informing content providers, exchanging information between operators etc.).

c) co-operation of operators with judicial and police authorities

Objective

To ensure effective cooperation between operators and the judicial and police authorities within Member States in combating the production and circulation of illegal content offensive to human dignity in audiovisual and on-line information services.

The codes of conduct should address, for example, the issue of basic rules on co-operation procedures between operators and the competent public authorities, while respecting the principles of proportionality and freedom of expression as well as relevant national legal provisions.

2.2.3 Violations of the codes of conduct

Objective

To strengthen the credibility of the code (or codes) of conduct, taking account of its voluntary nature, by providing for dissuasive measures which are proportionate to the nature of the violations. In this connection, provision should be made, where appropriate, for appeal and mediation procedures.

Appropriate rules to govern this area should be included in the code of conduct.

3. NATIONAL BODIES FACILITATING CO-OPERATION AT EUROPEAN UNION LEVEL

Objective

To facilitate co-operation at European Union level (sharing of experience and good practices; working together) through the networking of the appropriate structures within Member States, consistent with their national functions. Such structures could also allow international co-operation to be extended.

Co-operation at European level means:

- co-operation between the parties concerned:

all the parties involved in the drawing up of the national self-regulation framework are asked to set up a representative body at national level to facilitate the sharing of experience and good practices and to work together at European Union and International level.

- co-operation between national complaints-handling structures:

to facilitate and develop co-operation at European and International level, the parties involved in the centralised complaint management system are asked to set up a national contact point to strengthen co-operation in the fight against illegal content, facilitate the sharing of experience and good practices, and improve legal and responsible use of the networks.

4. EVALUATION OF SELF-REGULATION FRAMEWORKS

The objective is to provide for regular evaluations of the self-regulation framework at national level, to assess its effectiveness in protecting the general interests in question, to measure its success in achieving its objectives and to adapt it gradually to changes in the market, technology and types of use.

The parties concerned are asked to set up an evaluation system at national level so that they can monitor the progress made in implementing the self-regulation framework. This should take into account appropriate European-level co-operation, inter alia on the development of comparable assessment methodologies.